ARQUIVO
PARA A HISTÓRIA
DA TEORIA
DOS NÚMEROS
E DA LÓGICA

Editor Geral: John A. Fossa

TRATADO SOBRE A TEORIA DOS NÚMEROS EM XVI CAPÍTULOS

volume 8

Leonhard Euler

edufrn

Tratado sobre a Teoria dos Números em XVI Capítulos

Leonhard Euler
Tradução e Comentário de John A. Fossa

Tratado sobre a Teoria dos Números em XVI Capítulos

edufrn

Coordenadoria de Processos Técnicos
Catalogação da Publicação na Fonte.UFRN / Biblioteca Central Zila Mamede

Euler, Leonhard.
Tratado sobre a teoria dos números em XVI capítulos [recurso eletrônico] / Leonhard Euler ; John A. Fossa, tradução e comentário. – Natal, RN: EDUFRN, 2015.

1,13 Mb ; PDF

Modo de acesso: <www.repositorio.ufrn.br>
ISBN 978-85-425-0578-8

1. Teoria dos números. 2. Lógica matemática. 3. Matemática. I. Fossa, John A. II. Título.

CDD 512.7
RN/UF/BCZM 2015/71 CDU 511

Título Original: *Tractatus de numerorum doctrina capita sedecim, quae supersunt*.
Publicado em *Commentationes arithmeticae* 2, P. H. Fuss e Nicolaus Fuss (Es.), São Petersburgo: Academia Imperial de Ciências de São Petersburgo, 1849, p. 503-575.

Sumário

Introdução

O século XVIII, a exemplo dos que o precederam, bem como os que viriam subsequentemente, foi repleto de guerras no continente europeu. Não contente com o referido continente como palco da sua contenda, porém, os guerreiros europeus estenderam a luta a outras terras e outros povos, subjugando-os, no processo, à sua dominação. Em especial, a Inglaterra e a França se achavam numa disputa cerrada, que continuaria e se intensificaria no século XIX, para o que foi francamente visto como a dominação do mundo inteiro. Nem o generoso e bondoso matemático, Leonhard Euler, passou ileso desses acontecimentos, pois, para mencionar só a injúria mais tangível, uma propriedade rural dele na Prússia foi destruída por tropas russas.[1]

Houve ainda dois outros desenvolvimentos importantes que começaram no século XVIII e que continuariam, de uma forma ou outra, no século XIX. O primeiro foi um movimento filosófico, o Iluminismo, que até é usado hoje em dia para nomear o século XVIII como o "Século das Luzes". Falaremos

[1] No entanto, Euler seria recompensado posteriormente pelos próprios russos, devido à estima que estes tiveram para com o matemático suíço.

sobre isto mais adiante e, assim, aqui só mencionamos que a referida filosofia viu o homem como sendo perfectível através dos seus próprios esforços e, de fato, isto foi uma das principais influências no desenvolvimento da ideologia de progresso inexorável tão prevalente no século XIX.

Ainda mais, foi no século XVIII que aconteceu a primeira Revolução Industrial, sendo que a segunda começaria nos meados do século seguinte. É nessa primeira Revolução Industrial que problemas científicos e tarefas práticas da engenharia foram submetidos à análise matemática do novo cálculo infinitesimal, especialmente através do uso de equações diferenciais. Com referência a esse desenvolvimento, devemos observar que o próprio Euler foi um dos pioneiros na aplicação de equações diferenciais na maneira indicada.

Claramente os três desenvolvimentos aqui relacionados não foram acontecimentos independentes, mas não podemos explicar os seus entrelaçamentos no presente trabalho. Em vez disso, voltaremos a nossa atenção para a vida e obra de Leonhard Euler. Para tanto, dividiremos o resto da presente introdução em três partes, sendo a primeira dedicada a fazer alguns breves apontamentos sobre a vida de Euler, a segunda a uma revisão geral da sua obra e a terceira a uma explanação do texto *Tratado sobre a Teoria dos Números*, cuja tradução se

encontra no presente livro. Antes de proceder para os referidos itens, porém, apresentamos, em Figura 1, uma linha de tempo de Euler e alguns dos seus contemporâneos a fim de melhor situar o leitor referente a algumas das personagens importantes que atuavam no Século das Luzes.

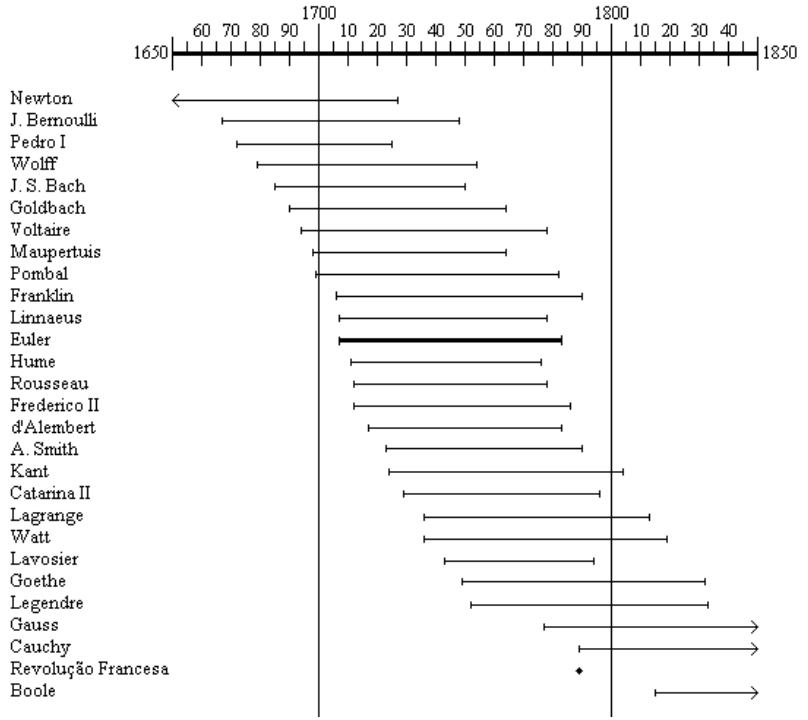

Figura 1. Linha do tempo de Euler e alguns contemporâneos.

Parte 1

Apontamentos sobre a Vida de Leonhard Euler[1]

No seu elogio de Euler, Nicolas Fuss[2] (2005, p. 2) inicia com a seguinte proposição chamativa:

> To understand the life of a great man, who has exemplified his century by enlightening the world, is to eulogize the human spirit.

Que Euler, um dos matemáticos mais produtivos de toda a história, foi um grande cientista é inegável. Mas, Fuss vai além disto, chama-o de um *homem* grande e virtualmente identifica-o como sendo o próprio espírito humano. Há, de fato, ampla razão para tanta retórica, pois Euler possuía não somente uma inteligência voltada para as intrigantes questões da matemática e

[1] Nessa seção, seguimos o relato de Fellmann (2007) e os fatos não atribuídos à outra fonte são retirados desta.

[2] Nicolas Fuss (1755-1826) foi um matemático suíço que emigrou para São Petersburgo em 1773 para atuar como secretário de Euler depois que este ficou quase cego. Atuou mais como um assistente do que como secretário, pois suas tarefas incluíam a resolução de problemas de pesquisa, o desenvolvimento das teorias de Euler, o cálculo de tabelas e a elaboração de exemplos. A partir de 1800, serviu, até seu falecimento, como secretário permanente da Academia de Ciências de São Petersburgo, onde seu elogio foi lido no dia 23 de outubro de 1783. Para mais detalhes sobre Fuss, ver O'Connor e Robertson (2006).

da ciência, mas também um profundo sentimento religioso e uma personalidade bondosa e simpática. Aliado a essas qualidades, Euler podia contar com uma memória quase fotográfica e um poder de concentração bastante desenvolvido, ambos postos a serviço de um comportamento caracterizado por, nas palavras de Emil Fellmann (2007, p. *xv*), "steady, quiet work." A propósito, B. F. Finkel (2007, p. 8) destaca o prazer que Euler sentia ao desenvolver trabalhos científicos:

> He was simple, upright, affectionate, and had a strong religious faith. His single and unselfish devotion to the truth and his joy at the discoveries of science whether made by himself or others, were striking attributes of his character.

Na verdade, vale a pena observar que a sua dedicação ao trabalho sério e constante faz parte da sua herança calvinista e, da mesma forma, a sua apreciação dos valores cristãos levou-o à prática da verdadeira caridade entre seus semelhantes.[3] Talvez possamos discernir nisto a integração dos vários aspectos da sua personalidade num todo harmonioso que ajudaria a explicar o fenômeno que foi Euler.

Seja como for, voltemos agora às palavras de Fuss, pois há nelas outro aspecto muito interessante, a saber, quando

[3] Por exemplo, numa época repleta de controvérsias sobre prioridades de descobertas científicas, Euler não somente recusava-se a de fazer recriminações desse tipo, mas foi, ao contrário, bastante generoso para com seus contemporâneos em respeito às suas próprias criações intelectuais.

afirma que Euler iluminou o mundo. A frase não é uma mera forma poética de se referir à quantidade ímpar de trabalhos científicos produzidos por Euler. É também uma referência clara ao próprio "Século das Luzes," isto é, como já mencionamos, o século caracterizado pelo Iluminismo,[4] uma filosofia que pretendia libertar o homem, através do uso da razão, da escravidão à superstição e às crenças irracionais. Assim, os Iluministas Franceses atacaram impiedosamente a religião, especialmente a religião organizada, como um obstáculo supersticioso ao desenvolvimento de formas mais justas de organização social. Isto, como já vimos, seria anátema para Euler. Entre os Iluministas Alemães, no entanto, os ataques contra a Igreja foram minimizados e, em qualquer caso, Fuss não foi um filósofo profissional e, portanto, simplesmente desconsiderava esse aspecto da referida filosofia, concentrando-se, em vez disto, na doutrina central de que o homem poderia engendrar o progresso da espécie através do uso da razão para resolver os problemas sociais. Neste sentido, o século XVIII fervia com o desenvolvimento da ciência aplicada e a tecnologia que faziam inovações transformadoras nas áreas de produção

[4] Observamos que o termo "Iluminismo" para referir à filosofia dominante do século XVIII só se tornaria generalizado entre os franceses e ingleses nos meados do século XIX. Não obstante, o termo paralelo alemão, *Aufklärung*, foi popularizado muito antes.

industrial, comunicação e transportação, entre outros. Isto, é claro, foi possibilitado pela aplicação da matemática, especialmente o cálculo infinitesimal e equações diferenciais, a problemas práticos e, como já vimos, Euler foi um dos primeiros que desenvolveu tais investigações. Desta forma, Fuss virtualmente identifica Euler com o *Zeitgeist* do Século das Luzes, com sua confiança no progresso ilimitado do homem através dos seus próprios esforços racionais.

Voltemos nossa atenção, então, para alguns dos detalhes da vida de Euler. Para tanto, organizaremos os eventos históricos, como faz a maior parte dos seus biógrafos, em quatro períodos, determinados pelos locais em que vivia em cada época. Especificando, o primeiro período, de 1707 a 1727, compreende a sua juventude na sua cidade natalícia, a Basileia; o segundo período, de 1727 a 1741, corresponde a primeira estadia de Euler em São Petersburgo; o terceiro, que vai de 1741 a 1766, abrange o tempo em que permaneceu em Berlim; o quarto, de 1766 a 1783, corresponde a sua segunda estadia em São Petersburgo.

A Juventude de Euler em Basileia

A etimologia do nome Euler é frequentemente relacionada à palavra alemã *Aul*, que significa “argila” (isto é, o

barro usado para fazer potes) e, portanto, indica a profissão de olaria. Segundo Fellmann (2007), portanto, o nome é encontrado em documentos que remontam até o século XIII e significa "dono de um pequeno prado." Ainda segundo o referido autor, a família vivia perto da Lagoa de Constância (*Bodensee*) e era chamada Euler-Schölpi até Hans-Georg Euler (1573-1663) mudou-se para Basileia e suprimiu a segunda parte do nome da família. O nome *Schölpi* significa "vesgo" ou "estrábico" e Ronald S. Calinger (2007) sugere que isto poderá indicar que problemas com a visão era muito frequente na família Euler. Como veremos mais adiante, o próprio Leonhard padeceria de problemas sérios com a visão.

Basileia foi originalmente uma vila celta, mas, devido à sua localização estratégica no Reno, foi conquistada pelos romanos. Por vários séculos, foi governado por uma série de bispos, um dos quais, no início do século XIII, construiu o que foi, por muito tempo, a única ponte sobre o Reno. A ponte contribuiu para o crescimento econômico e político da cidade, que, em 1501, foi incorporada à Suíça. A cidade se tornou referência na atividade da publicação de livros e como um centro humanístico, sendo que a Universidade de Basileia, a mais antiga da Suíça, foi fundada em 1459.

Figura 2. Leonhard Euler, 1737.[5]
Fonte: O'Connor & Robertson (2008).

O pai de Euler, Paulus Euler (1670-1745), estudou na Universidade de Basileia e eventualmente foi ordenado um ministro calvinista. Mesmo assim, sua posição econômica foi bastante precária até sua promoção, em 1708, à posição de pastor da igreja em Riehen, uma pequena vila na vizinhança de Basileia. Ao contrário da família Euler, a família da sua mãe, Margaretha Brucker (1677-1761), incluía vários estudiosos de certa importância, especialmente no campo das artes e letras. O próprio Euler nasceu no dia 15 de abril de 1707, sendo o primogênito do casal Paulus e Margaretha Euler. O casal ainda

[5] A datação das imagens de Euler segue Fasanelli (2007).

teve três outros filhos, a saber, Anna Maria (1708-1778), Maria Magdalena (1711-1799) e Johann Heinrich (1719-1750).

Paulus Euler cuidava dos primeiros passos na educação do seu filho, mas eventualmente o jovem Euler passou a fazer a viagem diária[6] (de aproximadamente uma hora) para Basileia para estudar na escola do município. Visto, porém, que a escola pública da época deixava a desejar, Paulus também contratou um tutor particular para seu filho. O tutor, Johannes Burckhardt (1691-1743), foi um teólogo, mas também, como o próprio Paulus Euler, gostava muito da matemática. Segundo Fellmann (2007), Burckhardt deveria ter exercitado uma grande influência sobre o jovem Euler, embora isto não fosse, até agora, esclarecido de forma satisfatória.

Como era costume da época, Euler, aos treze anos de idade, entrou no curso preparatório (mais ou menos correspondente ao nosso segundo grau) da Universidade de Basileia com o intuito, conforme os desejos dos seus pais, de estudar a teologia e seguir na careira do Euler pai. Ao final dos dois anos desse curso, escreveu uma espécie de trabalho final de curso, intitulado *De temperantia* e ingressou na Escola de Teologia da Universidade.

[6] Isto é relatado por Fellmann (2007). Mesmo assim, na sua pequena autobiografia, contida na própria obra de Fellmann, Euler afirma que morava com sua avó em Basileia nesse período.

Ainda no primeiro ano no curso preparatório, no entanto, Euler havia cursado a disciplina obrigatória de Johann I Bernoulli[7] (1667-1748) sobre geometria e aritmética. Isto, junto com a crescente amizade que travou com os filhos de Bernoulli, parece ter aguçado seu já apurado gosto pela matemática. Assim, pleiteou do mestre lições particulares. Bernoulli, contudo, ostensivamente devido à grande quantidade de suas tarefas oficiais, negou a Euler esse obséquio, mas consentiu a indicar para ele certas leituras e recebê-lo aos sábados à tarde para tirar as suas dúvidas. Os encontros com Bernoulli continuaram quando Euler entrou na Escola de Teologia e, eventualmente, ele, com a ajuda de Bernoulli, convenceu seu pai a permiti-lo mudar para o Curso de Matemática. Aparentemente, Paulus Euler nem ofereceu muita resistência à referida mudança, pois ele próprio gostava da matemática e, como O'Connor e Robertson (1998) observam, Bernoulli foi um amigo de Paulus quando os mesmos haviam cursado a Universidade na mesma época.

O acolhimento de Euler por Bernoulli é, de certa forma, extraordinário, pois Bernoulli era reconhecido pelos seus pares

[7] A família Bernoulli produziu vários matemáticos e cientistas de eminência. Infelizmente, a família não foi muito criativa na escolha de nomes dados e, assim, como se faz para reis e papas, tornou-se costume de afixar algarismos romanos aos mesmos para distinguir entre os xarás.

como o proeminente matemático da época. Mais ainda, era um homem de difícil convivência, sendo briguento, desconfiado e quase insanamente ciumento da sua posição como o primeiro entre os matemáticos. Mesmo assim, não somente salvou o jovem Euler de seu afogamento na teologia, mas também proferiu a ele a oportunidade de aprimorar suas habilidades nativas com instruções que eram desafiantes e, ao mesmo tempo, incentivadoras.

Euler correspondeu à tutela de Bernoulli com dedicação e apego, concluindo seus estudos universitários em 1726. Nesse mesmo ano, submeteu um trabalho à Academia de Paris, que promovia uma competição que premiaria o melhor ensaio investigativo sobre a maneira mais eficaz de arranjar os mastros em embarcações marítimas. O trabalho de Euler não ganhou o prêmio, mas a Academia o distinguiu com a avaliação *accessit* ("está perto"), que nas palavras de O'Connor e Robertson (1198, p. 2), "was a fine achievement for the young graduate." O trabalho é bastante interessante noutro sentido, como avalia Fellman (2007, p. 20)[8]:

> [...] Highly characteristic of EULER's attitude toward nature is the proud, final paragraph of this work: *I did not find it necessary to confirm this theory of mine by experiment, because it is derived from the surest and*

[8] Ênfase no original. O autor também indica, numa nota, que a tradução do trecho citado do artigo de Euler foi feito por O. Spiess.

> *most secure principles of mechanics, so that no doubt whatsoever can be raised on whether or not it be true and takes place in practice*.
> This almost blind confidence in the rigor of principles and in the a priori deductions accompanied EULER to his old age and characterizes a paradigm of his creative work.

No entanto, a avaliação de Fellmann sobre a confiança que Euler havia depositado aqui no método dedutivo da matemática poderá ser exagerada, pois certamente teria sido quase impossível para Euler, que morava no interior da Europa e nem havia visto um navio marítimo, a providenciar semelhantes experimentos; assim, podemos entender a afirmação de Euler como uma racionalização para a falta de experimentos.

No ano seguinte, 1727, Euler escreveu uma monografia sobre a acústica e a submeteu ao processo seletivo para preencher a posição de professor de física na Universidade de Basileia. O referido processo consistia de duas fases. Na primeira, as três melhores monografias foram selecionadas pela comissão de seleção, enquanto, na segunda, o ganhador foi determinado por um sorteio. Presumivelmente Bernoulli tentou interferir a favor de Euler, mas a sua influência não foi o suficiente a levar o nome do seu aluno à fase do acaso. Desta forma, Euler aspirava ir à Rússia, onde uns filhos de Bernoulli haviam conquistado umas posições na corte do Pedro, o Grande.

A Primeira Estadia em São Petersburgo

O filho mais velho de Bernoulli era Nicolaus II Bernoulli (1695-1726). Estudou direito e matemática, passando a ser, por certo tempo, assistente do seu pai. Seu irmão, Daniel I Bernoulli (1700-1782) foi designado por seu pai a ser um homem de negócios, mas, a exemplo do próprio Johann, que havia contrariado planos idênticos do seu pai em relação a si, Daniel insistiu em estudar a matemática. Johann, no entanto, procurava um ofício mais lucrativo para o filho e, no final das contas, concordaram que Daniel estudaria medicina. Fiel à sua vocação, Daniel, na sua tese de doutorado, aplicou conceitos matemáticos e físicos à medicina.

Figura 3. Leonhard Euler, 1753.
Fonte: O'Connor & Robertson (2008).

Os dois irmãos Bernoulli obtiveram, em 1725, posições como professores na nova Academia de São Petersburgo. Fruto do empenho de Gottfried Wilhelm Leibniz (1646-1716) que sonhava com uma série de academias eruditas nos principais países europeus, a Academia havia sido fundada pelo czar Pedro I, O Grande, em 1724. Pedro I havia derrubado a potência regional, a Sueca, na Guerra Nórdica, o que aumentou seu território, e seus cofres, consideravelmente. Assim, construiu uma nova capital para seu império em São Petersburgo, onde, depois de ter conversado com Leibniz, sediou a nova Academia. Faleceu antes de completar o projeto, mas a sua esposa, Catarina I, que se tornou czarina, prosseguiu com o mesmo.

Na época, a Rússia era um país quase medieval, com uma corte esplêndida e a maior parte da população escravizada. Dessa forma, não se encontrava no país uma quantidade suficiente de intelectuais qualificados para compor a proposta Academia. Em consequência, o czar convidou eminentes pensadores estrangeiros a preencher posições atrativas da nova instituição. Para o primeiro presidente, convidou, de fato, Christian Wolff (1679-1754), que, depois de Leibniz, era um dos mais conhecidos filósofos da Europa. Esse, no entanto, junto com Johann Bernoulli, outro convidado, recusou o convite. Tanto Wolff, quanto Bernoulli, recomendaram os irmãos

Bernoulli ao czar. Euler, como já vimos, era muito amigo dos referidos irmãos, especialmente de Daniel, e, não obtendo sucesso no concurso para a posição na Universidade de Basileia, pleiteou uma posição na Academia russa. Apoiado pelos três Bernoulli, pai e dois filhos, Euler foi chamado a São Petersburgo, aonde chegou em 1727 para ensinar matemática e física aplicadas à fisiologia, um assunto sobre o qual sabia pouco. Felizmente, na sua chegada, que por azar coincidiu com o falecimento de Catarina I, conseguiu mudar o ofício para o ensino de física.

Por não ser uma das posições mais altas, a remuneração de Euler não foi das melhores e, portanto, residiu na casa do seu amigo Daniel Bernoulli, com quem também colaborava em vários projetos científicos, especialmente na área de mecânica de fluidos. São Petersburgo, contudo, não agradava ao Bernoulli e, quando ele partiu em 1731, a cátedra de matemática que ele havia recebida no ano anterior, foi dada a Euler. O resultante melhoramento na sua situação financeira lhe proporcionou a estabilidade necessária de criar uma família e, no início de 1734, casou-se com Katharina Gsell (1707-1773), filha do artista Georg Gsell (1663-1740) de Basileia, com quem teve treze filhos, embora oito deles faleceriam na infância.

Euler, como era de seu costume, trabalhava diligentemente durante esse período. Em recompensa, ele teve a oportunidade não somente de colaborar com Daniel Bernoulli, mas também de conviver com um grupo de brilhantes cientistas, pensadores e artistas.[9] Entre esses estava o diplomata e matemática Christian Goldbach (1690-1764), o primeiro secretário permanente da Academia, cuja fama hodierna é principalmente associada à Conjectura de Goldbach[10]. Um espécie de Mersenne[11] do século XVIII, Goldbach manteve uma correspondência extensiva com os matemáticos da época e repassou muitos problemas intrigantes para Euler, pois os dois ficaram grandes amigos. Enquanto isso, Euler também manteve uma correspondência científica com seu mentor Johann Bernoulli e ainda achou tempo de apreender a língua russa, o que foi bastante raro entre os membros estrangeiros da Academia.

Em 1738, Euler ficou cego de um olho – o olho direito – e os seus contemporâneos, bem como o próprio Euler, seguindo os padrões médicos da época, atribuíram a ocorrência ao seu

[9] Segundo Peter Hoffmann (2007), Euler foi ciente – e bastante apreciativo – disto.
[10] Todo inteiro par maior que 2 pode ser representado como a soma de dois primos.
[11] Frade Marin Mersenne (1588-1648) manteve correspondência com os principais matemáticos da sua época, entre os quais foram Pierre Fermat (1601-1665) e Blaise Pascal (1623-1662), noticiando resultados e repassando desafios.

hábito de trabalhar quase excessivamente. Robin Wilson[12] (2002, p. 5) rebate essa explicação da seguinte forma:

> Although he attributed it to overwork, particularly for some close work that he had been doing on cartography, it was more probably due to an eye infection.

De fato, Euler havia sofrido uma infecção, acompanhada por uma febre altíssima alguns anos antes, em 1735, que quase o matou. Fellmann (2007) sugere que a doença que levou à perda do olho foi relacionada com essa infecção anterior. Visto que houve três anos entre os dois acontecimentos, contudo, é mais provável que tenha contraído uma nova infecção. Seja como for, o jovem matemático continuou a trabalhar em seu ritmo frenético.

Com o passar dos anos, no entanto, a instabilidade política no estado russo, iniciada com o falecimento de Pedro I, cresceu muito. Somado a isto, os nacionalistas russos conseguiram mais concessões para seu projeto de "russificação", ou seja, a imposição da cultura propriamente russa, em detrimento à cultura emprestada da parte oeste da Europa (certos nobres russos, por exemplo, preferiram falar, no dia a dia, francês em vez de russo). Dessa forma, a situação começou a se complicar para os estrangeiros no império e, portanto, Euler decidiu sair da sua posição na Academia de São Petersburgo.

[12] Wilson (2007) contém basicamente o mesmo material.

Nem todos, porém, concordam com a explicação dada no parágrafo anterior, pois, alegam que Euler, devido à estima que havia conquistado dentro da Academia, não seria afetado pelas circunstâncias relatadas. A isto, podemos acrescentar que o fato de que ele havia apreendido a língua russa deveria ter aumentado a sua aceitabilidade a todas as frações do mosaico russo e, na verdade, isto é comprovado pelo fato de que, quando ele decidiu aceitar o convite de Frederico II, o Grande, a vir para Berlim, o presidente da Academia de São Petersburgo, o autocrático Laurentius Blumentrost (1692-1755), quase conseguiu impedir a sua saída, embora não teve a autoridade legal para tanto. Assim, Fellmann (2007) argumenta que, de fato, foi a sua esposa, Katharina, que o convenceu a aceitar o convite de Frederico, pois ela temia os fogos que atormentavam a capital russa. Visto que as casas foram construídas de madeira e situadas perto umas às outras, aconteciam, de tempos em tempos, grandes conflagrações que destruíam centenas de casas de uma só vez. Acrescentada a esse perigo foi a frequente inconveniência de precisar acomodar, no seu lar, soldados russos devido à falta de instalações militares adequadas na nova capital.

Embora não seja possível determinar agora a relativa importância desses motivos para a sua partida, o certo é que Euler partiu para Berlim em 1741.

A Temporada de Euler em Berlim

O motivo do convite de Frederico II (1712-1786) a Euler foi seu desejo de fundar uma academia de ciência em Berlim. Já existia uma Sociedade para as Ciências, formada com a ajuda de Leibniz, mas ela se achava desamparada devido ao descaso – para não dizer desdém – de Frederico Wilhelm I (1688-1740), seu predecessor como Rei da Prússia.[13] Agora, porém, Frederico II queria uma academia que pudesse superar as três instituições mais importantes desse tipo: a Academia Real de Londres, a Academia de Paris e a Academia de São Petersburgo. Para tanto, queria convidar o filósofo francês François Voltaire (1694-1778) para ser presidente da nova instituição, mas, quando viu que o mesmo não aceitaria o convite, voltou-se para Christian Wolff e Pierre-Luis Maupertuis (1698-1759), o matemático francês, como co-presidentes e Johann Bernoulli como chefe do setor de matemática. Wolff e Bernoulli não aceitaram o convite e, assim, Maupertuis ficou como presidente, enquanto Euler, que havia ganhado o grande prêmio da Academia de Paris em 1738 e 1740, foi apontado como chefe do setor de matemática e substituía Maupertuis nas ausências deste. Os dois ficaram amigos e Euler se tornou uma espécie de eminência parda na

[13] Prússia, localizada ao norte da Alemanha, foi o principal estado do Império Alemão. O Império foi fundado pelos Brandemburgo em 1701 e durou até 1918.

direção da nova academia, embora Winter, *apud* Fellmann (2007, p. 90) cita uma carta de Maupertuis em que refere a Euler como “intrometido”.

Figura 4. Leonhard Euler, 1756.
Fonte: O’Connor & Robertson (2008).

Apesar do seu interesse em estabelecer uma nova academia, Frederico atuava mais por motivos de promover o esplendor do seu reinado do que interesse sincero na ciência. De fato, entendia pouco sobre a matemática e a ciência, embora apreciasse sua utilidade para sua atividade predileta, a guerra, e, desta forma, mesmo seus convidados chegando a Berlim em 1741, a fundação da Academia só aconteceria em 1744, quando

houve uma pequena pausa nas suas atividades bélicas. Embora Frederico, como veremos a seguir, não tratava seu matemático chefe inteiramente bem, Euler ficou bastante feliz no início da sua temperada em Berlim, onde ficaria por 25 anos, inclusive mantendo durante todo esse período uma correspondência com o rei, cuja capital foi locada em Potsdam, quase 30 quilômetros distante de Berlim.

Enquanto permanecia na Prússia, Euler produziu obras clássicas sobre o cálculo de variações, a balística, o cálculo diferencial e integral (incluindo o início da teoria de funções), a óptica e xadrez. Ainda compôs, na língua francesa, as *Cartas a uma princesa alemã*, uma exposição quase filosófica dos seus pensamentos defendendo o cristianismo e incluindo muita divulgação científica. De fato, Breidert (2007, p. 100) observa que

> In philosophy Euler takes up the pen only in cases where he is convinced that he has to protect the Holy Bible or the sciences against philosophers' attacks or against their false doctrines.

Em todo caso, a obra, publicada em São Petersburgo, foi um grande sucesso. De fato, o local da publicação das *Cartas* ilustra o fato de que Euler ainda colaborava com a Academia de São Petersburgo, não somente submetendo vários artigos à sua revista, mas também utilizando a pensão que recebia dessa

instituição para comprar livros e instrumentos científicos a serem remetidos a ela. Também foi encarregado por Frederico a participar de vários projetos práticos, entre os quais podemos mencionar projetos hidráulicos, melhoramentos na produção de seda e aperfeiçoamentos no processo da cunhagem de moedas.

A propósito dos projetos práticos mencionados no parágrafo anterior, há o caso polêmico do sistema hidráulico de Sanssouci. Frederico queria construir uma rede imponente de fontes e cascatas artificiais no local do seu novo palácio em Sanssouci na cidade de Potsdam. A fonte principal teria um jato d'água que se elevaria uns trinta metros no ar. Para obter esse efeito, era necessário construir uma grande caixa d'água numa colina uns 50 metros acima do nível do rio que iria alimentar o sistema. Euler se associou a esse projeto, que fracassou de modo espetacular. Vários historiadores veem nisto evidências de que Euler, embora fosse um matemático teórico ímpar, tinha pouca habilidade na matemática aplicada. No entanto, dadas as suas realizações nesta área da matemática, isto certamente é, no mínimo, um julgamento apressado e, assim, devemos considerar outras explicações.

Na verdade, Michael Eckert (2002) argumenta, de forma bastante contundente, que Euler não estava responsável pelas obras de Sanssouci, mas agiu apenas como uma espécie de

consultor. Mais ainda, Euler fez certas especificações e recomendações, como o uso de canos metais em vez de canos de madeira, para a construção e até previu que a consequência de não seguir as suas instruções seria a destruição da obra pela força da própria água nela usada. Os responsáveis pelo projeto, contudo, tinham pouca experiência com construções hidráulicas e desconsideraram as recomendações de Euler, o que resultou, naturalmente, na plena realização da previsão do matemático suíço. Eckert (2002) também indica que uma parcela considerável da culpa para o fracasso das obras hidráulicas em Sanssouci pertence ao próprio rei, pois, embora alimentasse planos espantosos, era demasiadamente mesquinho na hora de apoiá-los financeiramente.

Seja isto como for, porém, vamos agora voltar aos acontecimentos na Academia em Berlim. Com o falecimento de Maupertuis em 1759, Euler esperava obter a presidência da academia prussiana, pois não foi somente um cientista bastante superior a Maupertuis, mas também estava virtualmente dirigindo, dos bastidores, a mencionada instituição. Segundo Fellmann (2007), Frederico queria, para o presidente da Academia, um homem urbano e sofisticado – alguém que se sentiria confortável na companhia dos membros refinados da corte – e o probo Euler, que aos olhos do rei foi nada mais que

uma máquina de calcular, simplesmente não correspondia ao perfil exigido. Frederico, porém, lhe permitiu continuar a presidir a Academia na prática, mas não lhe agraciou formalmente com o título – e o consequente aumento salarial – desejado. Com isto, Euler decidiu voltar à Academia de São Petersburgo, o que aconteceu em 1766.

Há, no entanto, ainda mais a ser contado sobre a saída de Euler de Berlim, pois o próprio Euler, em 1748 – portanto quase no início de sua temporada na Alemanha – já estava à procura de uma posição na Academia Real de Londres que poderia lhe render um salário melhor. Mas parte considerável da sua atitude foi consequência da sua relação com o rei prussiano que o considerava como um súdito, sujeito aos caprichos reais. Por sua vez, Euler, embora nunca mais houvesse voltado para a sua pátria[14], se identificava como cidadão suíço e, portanto, como um homem livre; deste ponto de vista, a Inglaterra ofereceria um ambiente[15] muito mais agradável às suas expectativas. O desfecho da sua estadia em Berlim fortalece essa interpretação, pois, quando pediu ao rei exoneração do seu ofício para poder

[14] Calinger (2007) relata que, nesse mesmo ano de 1748, com o falecimento de Johann Bernoulli, foi oferecida a Euler a cadeira do seu ilustre mestre na Universidade de Basileia. No entanto, ele não se interessou em ingressar na universidade, pois a posição numa academia nacional era mais prestigiada e lhe proporcionava mais tempo livre para dedicar-se à pesquisa.

[15] A Sociedade Real de Londres, ao contrário das academias de Paris, São Petersburgo e Berlim, não foi controlada pelo governo.

voltar a São Petersburgo, Frederico respondeu imperiosamente que não queria conversar sobre isto. Assim, Euler fez uma espécie de greve, deixando de trabalhar e de assistir as sessões da Academia, o que, no entanto, deveria ter sido mais penoso para o próprio Euler do que para o rei. Depois de seis meses – e a mediação de terceiros, notavelmente Jean le Rond d'Alembert[16] (1717-1783) – Euler obteve permissão de deixar Berlim, mas também teria de deixar seu filho, Christoph (1743-1808), um oficial do exército prussiano; levaria mais uns seis meses para este obter permissão a rever sua família.

A Segunda Estadia em São Petersburgo

Durante os 25 anos que Euler havia ficado em Berlim, a situação na Rússia se estabilizou com a ascensão de Catarina II, a Grande, (1729-1796) ao trono em 1762. Euler, contudo, não aceitou voltar a São Petersburgo sem negociar um pacote de vantagens, incluindo um bom aumento na sua remuneração, isenção do requerimento geral de alojar militares na sua residência e uma posição como Professor de Física para seu filho Johann Albrecht; também queria posições para outros dois

[16] Embora o matemático francês d'Alembert houvesse alguns desentendimentos com Euler, aconselhou Frederico a deixar o suíço partir para evitar escândalos. Frederico, que queria que d'Alembert aceitasse a presidência da Academia, muito a desgosto de Euler, finalmente aquiesceu. Antes que Euler deixasse Berlim, d'Alembert, em visita à cidade, encontrou com o mesmo e os dois se tornaram amigos.

filhos, Karl e Christoph, como, respectivamente, médico e militar[17]. Com a exceção da primeira, Catarina aceitou as exigências de Euler e, assim, este concordou em voltar à Rússia. Na viagem de volta para São Petersburgo, o matemático suíço foi recebido por vários nobres, notadamente o Rei Stanislas da Polônia, que, nas palavras de André Weil (2007, p. 48), "treated him almost like a fellow-sovereign." Quando chegou a São Petersburgo, também foi recebido acaloradamente pela czarina[18], a qual logo confiou a ele a tarefa de reerguer a academia russa, que se encontrava num estado de decadência devido ao desinteresse e maus cuidados dos governos anteriores.

Em 1771, o que a sua esposa Katharina tanto receava aconteceu. Um grande incêndio destruiu a casa de Euler e a família só escapou sem ferimentos devido à ação enérgica para fugir. Condorcet (2005) ainda revela que Peter Grimm, um compatriota de Euler, entrou na casa já em conflagração e salvou o matemático cego, carregando-o para fora da casa nas costas. Dos seus bens, salvou-se apenas a maioria dos manuscritos de Euler. A czarina, no entanto, lhe concedeu uma nova casa. Alguns meses depois deste acontecimento, Euler se submeteu a uma operação para remover uma catarata do olho

[17] Condorcet (2005) alega que a verdadeira razão para a qual Euler voltou para São Petersburgo foi a de assegurar esses empregos para seus filhos.
[18] Segundo Calinger (2007), houve até os que queriam, na corte de Catarina, admitir Euler à classe dos nobres. A czarina, portanto, recusou, alegando que a sua fama já era maior que qualquer título de nobreza.

esquerdo. A operação foi bem sucedida, mas desenvolveram-se complicações pós-operatórias que o deixaram quase cego. Fuss (2005) relata que as referidas complicações deviam-se ao fato de que Euler não seguiu as ordens médicas no período de convalescença, voltando aos seus trabalhos antes do que deveria. Seja como for, a visão do matemático foi seriamente comprometida, ao ponto de que não poderia discernir, por exemplo, as fisionomias das pessoas em situações sociais, nem ler textos impressos. Poderia, no entanto, escrever e fazer cálculos numa prancha com giz e, com a ajuda de seus assistentes, especialmente seu filho Johann Albrecht e o já mencionado Nicolas Fuss, continuou a fazer suas pesquisas em matemática e em áreas conexas.

Figura 5. Leonhard Euler, 1778.
Fonte: O'Connor & Robertson (2008).

O falecimento da sua esposa Katharina veio a acontecer em 1773 e deixou Euler desamparado em relação ao gerenciamento das questões domésticas. Para não ficar dependente dos seus filhos, resolveu casar-se com uma viúva do seu conhecimento, Frau Metzen. Os filhos (já adultos) de Euler, contudo, observando que a proposta madrasta não era da sua classe social e, mais importante, temendo uma diminuição no tamanho da sua herança, conseguiram desfazer os planos do seu pai. No entanto, Euler, mostrando a resolução característica dele, arranjou outra noiva, Salome Abigail Gsell, meio-irmã (por parte do pai) mais moça da sua primeira mulher, e, apesar da oposição violenta dos seus filhos, o casal contraiu núpcias em 1776. Felizmente, logo depois do casamento, os filhos acabaram aceitando a nova situação e a paz voltou a reinar no lar dos Euler.

Ainda conta-se uma curiosa estória sobre Euler que teria acontecido durante sua permanência na corte de Catarina II. Segundo a versão dado por E. T. Bell (1937), o filósofo e ateísta francês Dinis Diderot (1713-1784), em visita à referida corte, passava dos limites com suas pregações ateístas e a czarina confiou a Euler a incumbência de abrandar o incômodo. Assim, o matemático suíço teria desafiado seu colega francês, segundo Bell (1937, p. 147), da seguinte maneira: "*Sir*, $\frac{a+b^n}{n}=x$, *hence*

God exists; *reply*!" Diderot, ignorante da álgebra e humilhado publicamente, voltou à França às pressas. B. H. Brown (2007), no entanto, observa que, de fato, Diderot possuía muito conhecimento matemático, tendo até publicado cinco trabalhos competentes sobre esse assunto, e, portanto, não teria sido enganado por um sofismo tão evidente. Em apoio à conclusão de Brown, podemos acrescentar que o suposto acontecimento não parece combinar com o que sabemos da personalidade de Euler – nem é verossímil que Catarina precisaria recorrer a Euler para se livrar de Diderot! Brown ainda sugere que a estória fora originada na corte de Frederico II que detestava o referido filósofo francês. Isto, sim, é verossímil, pois o rei prussiano foi adepto da zombaria; Fellmann (2007) relata que humilhava o próprio Euler, chamando-o de "meu pequeno ciclope", em referência a sua deficiência visual.

Não obstante os problemas com a sua visão, Euler, amparado pela nova esposa, os filhos e seus assistentes, continuou a prosseguir nos seus estudos, trabalhando até o dia 18 de setembro de 1783, dia do seu falecimento. Nesse dia, passou algum tempo com os netos, investigou, com seus assistentes, a órbita do recém-descoberto planeta Urano e, no fim da tarde, sofreu um derrame o que o levaria à morte algumas horas mais tarde.

Parte 2:

Revisão Geral da Obra de Euler

Euler foi certamente um dos mais prolíficos matemáticos de todos os tempos. Sua obra consiste em mais do que 800 artigos e livros, bem como uma correspondência científica de mais que 3000 cartas. Segundo Truesdell (2007, p. 15),

> Approximately one third of the entire corpus of research on mathematics and mathematical physics and engineering mechanics published in the last three quarters of the eighteenth century is by him.

Foi um grande inovador na Teoria dos Números, no Cálculo das Variações e na Análise Infinitesimal, especialmente na análise e aplicação de equações diferenciais. De fato, Calinger (1996, p. 129-130) relata que já no início do primeiro período que passou em São Petersburgo,

> The core of his research program was now set in place: number theory; infinitary analysis including its emerging branches, differential equations and the calculus of variations; and rational mechanics.

Mas, mesmo assim, não se limitou a esses assuntos, como podemos ver das seguintes porcentagens calculadas por

Adolf Pavlovich Yushkevich (*apud* Fellmann, 2007, p. 135-134) dos 760 itens editados até a data da compilação:

algebra, number theory, analysis	40%
mechanics and the rest of physics	28%
geometry, including trigonometry	18%
astronomy	11%
naval science, architecture, ballistics	2%
philosophy, music theory, theology and what is not included above	1%

Na matemática pura, os seus trabalhos de maior destaque são os que tratam de Séries Infinitas, o Cálculo Diferencial e Integral, Equações Diferenciais, Geometria Diferencial, Cálculo das Variações e a Teoria dos Números.

Ainda mais impressionante é a qualidade do seu trabalho. Criou várias subáreas importantes da matemática e ressuscitou, segundo Weyl (2001), a Teoria dos Números depois de encontrar alguns problemas investigados por Fermat. Ainda mais, ganhou o grande prêmio internacional da Academia de Paris doze vezes, mais do que qualquer outro matemática na história desse prêmio. Mesmo assim, Fellmann (2007) afirma que ele deveria ser creditado com ainda mais oito vitórias, pois, embora seu filho Johann Albrecht ganhasse o referido prêmio sete vezes e outro filho, Karl, uma vez, todos esses trabalhos premiados foram de fato de autoria do próprio Euler.

Referente ao seu modo de trabalho, Calinger (1996, p. 123) explica que

> After finding missing solutions, often by analogy, Euler returned periodically to perfect methods, make exhaustive computations, and systematize fields. His research signature is a patient, tenacious search in stages for greater precision, completeness, and taxonomic order.

Muitos dos seus artigos e livros revelam a mesma estrutura. Primeiro, apresentam-se vários exemplos numéricos que são subsequentemente comparados e dos quais conjecturas gerais são feitas. Por fim, apresentam-se demonstrações abstratas e estabelecem-se, quando apropriado, relações com outras áreas da matemática. Esta estrutura é bastante evidente nos seus trabalhos sobre a Teoria dos Números, o que faz esses trabalhos extremamente valiosos para a Educação Matemática.

Evidentemente, não podemos fazer uma revisão exaustiva da *obra* de Euler na presente introdução. Tentaremos, contudo, fazer uma pequena revisão de algumas das suas principais realizações.

O Cálculo

Antes de Euler, a análise era largamente concebida como o estudo de curvas. Euler, no entanto, mudou o foco, colocando a noção de função como primordial. Ao fazer isto, poderia

investigar as propriedades de curvas através de métodos puramente analíticos, o que lhe proporcionou técnicas mais poderosas e de mais generalidade. A necessidade para o conceito moderno de função, no entanto, ainda não se tornou evidente e, assim, Euler considerava funções como combinações algébricas de quantidades variáveis e constantes.

A diferencial *dx*, a diferença entre dois valores infinitamente próximos da variável *x*, era geralmente pensada como um número maior do que zero, mas menor que qualquer número positivo. A técnica básica era investigar $x+dx$ e, depois de manipular as expressões resultantes, eliminar as potências $(dx)^n$, para $n>1$, pois, visto que *dx* é infinitamente pequeno, suas potências seriam realmente desprezáveis. Euler, contudo, considerou essa formulação muito confusa e tentou superar o problema por conceber *dx* como um símbolo formal para o zero. Anthony P. Ferzola (2007) relata que Euler deduziu a fórmula $dx+(dx)^2 = dx$ por observar que $\frac{dx+(dx)^2}{dx} = 1+dx = 1$. A última equação é verdadeira, visto que, por definição, $dx = 0$. Segundo Jesper Lützen (2007), Euler pensava que "analysis was just infinite algebra" e isto nos dá algum *insight* ao pensamento de Euler. Aparentemente, pensava que o símbolo formal *dx* poderia ser manipulado livremente segundo as regras da álgebra. No

momento apropriado, porém, poderíamos substituí-lo por seu valor, 0, obtendo assim a resolução do problema. Esse procedimento, no entanto, não é mais claro que o método original. Mesmo assim, ele aplicou-o com desenvoltura e chegou a resultados inovadores. Na geometria diferencial, por exemplo, foi além do estudo de curvas, desbravado por Isaac Newton (1643-1727) e Jacob Bernoulli (1613-1727), iniciando o estudo de superfícies. Procurou a superfície de rotação mínima de todas as curvas do mesmo comprimento e mostrou que a superfície mínima é a gerada pela catenária. Segundo Karin Reich (2007, p. 481), "This was the first example of a minimal surface in history." É dada pela equação $dx = \frac{cdy}{\sqrt{(b-y)^2 - cc}}$.

Contribuiu para a busca para fórmulas de integração e introduziu fatores de integração na resolução de equações diferenciais. Ainda estudou integrais duplas. Nesse estudo, a integração da primeira variável frequentemente resulta em um novo integrando de difícil resolução. Euler descobriu que às vezes o mesmo poderia ser simplificado por uma troca de variáveis. Para efetuar esta troca, concebeu as variáveis *x* e *y* como funções de novas variáveis *u* e *v*. Assim, interpretou o produto das diferenciais *dx dy* como o elemento de área e o relacionou às diferenciais de *u* e *v* pela equação

$\left|\frac{\partial x}{\partial u}\frac{\partial y}{\partial v}-\frac{\partial x}{\partial v}\frac{\partial y}{\partial u}\right|dudv$, o que foi considerado como o elemento de área em relação às novas variáveis.

Outro importante conceito inventado por Euler é o da função gama. Segundo Sandifer (2007), Goldbach apresentou ao matemático suíço o problema de interpolação de fatoriais, que consiste em determinar o valor de *n*! para *n* racional. Isto é, pediu-se que determinasse o valor de, por exemplo, $\frac{11}{2}!$ Em seguida, Euler descobriu um produto infinito que é igual a *n*! e que permite a inclusão de argumentos não inteiros. Observou também que para $n = \frac{1}{2}$, o referido produto se reduz à equação $\left(\frac{2\cdot 2}{1\cdot 3}\right)\left(\frac{4\cdot 4}{3\cdot 5}\right)\left(\frac{6\cdot 6}{5\cdot 7}\right)\left(\frac{8\cdot 8}{7\cdot 9}\right)\ldots=\frac{\pi}{2}$, que havia sido descoberta por John Wallis (1616-1703), e isto lhe levou a procurar uma maneira de representar seu produto por uma integral. Descobriu que $n!=\int_0^1(-\log x)^n dx$, o que foi remanejado em $\Gamma(x)=\int_0^\infty e^{-t}t^{x-1}dt$ por Adrien-Marie Legendre (1752-1833).

Cálculo das Variações

O Cálculo das Variações é intimamente relacionado com a resolução de equações diferenciais, pois o problema geral é achar uma função minimal ou maximal que satisfaz uma

integral, geralmente junto com algumas condições iniciais. Já mencionamos a superfície mínima gerada pela catenária e, de fato, Euler usava métodos infinitesimais para abordar problemas variacionais. O matemático suíço publicou, em 1744, o livro *Método para achar curvas que gozam de uma propriedade máxima ou mínima, ou a solução do problema isoperimétrico, concebido no mais lato sentido*, que, apesar do título imponente, no julgamento de Carathéodory[1] (citado por Kreyszig, 2007, p. 210), "is one of the most beautiful mathematical works ever written." Nele se acha a *equação de Euler*, $\frac{\partial \mathrm{L}}{\partial y} - \frac{d}{dx}\left(\frac{\partial \mathrm{L}}{\partial y'}\right) = 0$, como uma condição sobre a função $y(x)$ para que a mesma seja uma solução da integral variacional $\mathrm{J}[y] = \int_{x_0}^{x_1} \mathrm{L}(x, y, y')dx$ com $y(x_0) = y_0$, $y(x_1) = y_1$ e $x_0 < x_1$.

Segundo Rüdiger Thiele (2007), a mencionada obra de Euler marcou o início da Teoria do Cálculo das Variações, pois antes só houve a resolução de problemas avulsos, enquanto Euler fez um estudo sistemático da nova área. Mesmo assim, porém, os métodos de Euler, ainda dependentes da geometria, foram, uns onze anos mais tarde, superados pelos métodos

[1] Constantin Carathéodory (1873-1950), matemático grego.

analíticos de Lagrange[2]. Euler reconheceu a superioridade do método de Lagrange e o incorporou nos seus trabalhos posteriores, até por volta de 1771, quando descobriu como reduzir esse método ao Cálculo Diferencial, fazendo assim uma simplificação enorme da teoria. Para mais detalhes, ver Thiele (2007).

Mecânica e Astronomia

Talvez a característica mais ressaltante da obra de Euler referente à aplicação da matemática à ciência é o uso de métodos infinitesimais. De fato, segundo Stacy G. Langton (2007), ele concebeu a ideia inovadora de aplicar a segunda lei de Newton (**F** = *M***a**) aos elementos infinitesimais de corpos em moção para determinar as leis de movimento. Inicialmente, queria basear toda a mecânica neste princípio, tomado como um axioma, mas eventualmente reconheceu que precisaria um princípio adicional referente ao momento de rotação. Ainda separou o componente do movimento devido à moção do centro de gravidade do componente devido à rotação do corpo ao redor do referido centro. Isto é muito evidente, por exemplo, na sua discussão do movimento de barcos no seu famoso livro *Ciência*

[2] Joseph Luis Lagrange (1736-1813), matemático francês, nascido na Itália.

naval, publicado em 1749, mas aparentemente escrito uns dez anos antes.

Foi o primeiro cientista a fazer uma formulação quantitativa do princípio de mínima ação e, segundo Teun Koetsier (2007), foi o primeiro a usar sistemas de coordenadas cartesianas ortogonais para descrever o movimento de corpos. A motivação original parece ter sido a simplificação dos cálculos complicados que resultaram do uso de sistemas cartesianos "intrínsecos". Para descrever as trajetórias pleiteadas, porém, ele usou dois sistemas, um fixo no espaço "absoluto" e o outro fixo ao corpo em movimento. Isto o levou a resolver o problema puramente matemático de descobrir as transformações relacionando as coordenadas de dois sistemas.

Na astronomia, já mencionamos a teoria lunar de Euler. Também trabalhou na área da determinação das órbitas dos planetas, especialmente em relação às perturbações observadas nelas. O maior exemplo disto foi as perturbações mútuas dos planetas Júpiter e Saturno, que, aliás, não conseguiu resolver de forma satisfatória. O problema o levou a desconfiar que o termo $\frac{1}{r^2}$ na lei de gravitação de Newton não fosse correto (Clairaut[3] e d'Alembert chegaram à mesma conclusão), mas Clairaut

[3] Alexis Claude Clairaut (1713-1765), matemático francês.

eventualmente mostrou que, em relação a certos movimentos da lua, a lei newtoniana foi correta e Euler aceitou o resultado como sendo definitivo. Desenvolveu uma teoria para explicar a precessão dos equinócios e, no processo, resolveu completamente o problema da rotação de corpos rígidos.

Séries Infinitas

Newton já havia mostrado que séries infinitas poderiam ser uma arma poderosa na resolução de problemas difíceis do Cálculo e nisso vários outros matemáticos, incluindo Euler, seguiram seu exemplo. Em especial, Euler usou séries para calcular, ou pelo menos aproximar, integrais para as quais não conhecia uma fórmula fechada e, segundo Victor J. Katz (2007, p. 216), "Euler claimed that any function can be expressed as an infinite series". Assim, por expressar uma função como uma série infinita, poderia integrar ou diferenciar termo por termo de forma bastante fácil. Também usou este recurso para calcular aproximações para tais constantes como π. Na verdade, o recurso era tão importante na matemática de Euler, que, como C. Edward Sandifer (2007) observou, ele publicou mais artigos sobre esse assunto do que qualquer outro, com a exceção da Teoria dos Números.

Uma das características da época foi o fato de que não se entendia bem a natureza de séries divergentes e as limitações que a divergência impõe na manipulação de séries. Assim, em relação à metodologia de trabalho do matemático suíço, Morris Kline (2007, p. 101) afirma que

> Like his predecessors, Euler's work lacks rigor, is often *ad hoc*, and contains blunders, but despite this, his calculations reveal an uncanny ability to judge when his methods might lead to correct results.

Por volta de 1755, no entanto, Euler vislumbrava algumas dessas dificuldades e argumentou explicitamente (embora o procedimento defendido não fosse original com ele) que, sempre que uma série é gerada por uma expressão fechada, ela pode ser somada por atribuir valores à variável da expressão. Reconheceu que isto é uma extensão do significado de "soma", mas pensou que os resultados assim obtidos seriam úteis. A técnica foi utilizada na soma da série alternada 1–1+1–1+1–1+..., uma série, aliás, que ocasionava muita controvérsia, visto que a soma parecia ser 0 ou 1, conforme fosse agrupado como (1–1)+(1–1)+(1–1)+..., ou como 1+(–1+1)+(–1+1)+(–1+1)+... Em contraste, o matemático italiano Guido Grandi (1671-1742), observou que

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots$$

Assim, ao fazer $x = 1$, obtém-se o resultado 1–1+1–1+1–1+... = $\frac{1}{2}$. Euler concordou com Grandi e ainda acrescentou que

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots,$$

de tal modo que, ao fazer $x = -1$, obtém-se o mesmo resultado. A soma $\frac{1}{2}$ também é achada por tratar a série como uma progressão geométrica e, desta forma, o fato de que vários métodos nos levam ao mesmo resultado é tido como forte evidência para a validade do mesmo. De fato, Euler usou esse critério na sua investigação da série hipergeométrica de Wallis[4]:

$$1–1!+2!–3!+...$$

Depois de aproximar a soma por quarto métodos distintos, ele constatou que a série converge e que a sua soma é por volta de 0,59.

Euler também trabalhou com o que seria conhecido como a "função zeta":

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

[4] A série é chamada "hipergeométrica" porque cada termo é obtido do precedente por multiplicar por um fator diferente. Segundo E. J. Barbeau (2007), a referida série não se encontra na obra de Wallis e a razão para a qual Euler a atribuia ao Wallis é um mistério.

Para s = 1, se obtém a série harmônica, que se sabia ser divergente. Para s = 2, se obtém o problema de Basileia: determinar a soma de

$$\frac{1}{1}+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots$$

Os Bernoulli havia determinado que a série converge e se empenhavam em estabelecer limites sempre mais estreitos dentro de que a soma se situava. Euler, no entanto, resolveu o problema quando mostrou que a sua soma é igual a $\frac{\pi^2}{6}$.

De posse de várias somas, manipulou as séries para determinar as somas de outras. Não entraremos nos detalhes aqui. Simplesmente mencionamos, sem maiores comentários, alguns dos seus resultados relacionados a séries infinitas: números de Bernoulli, números de Euler, a constante γ, a constante Euler-Mascheroni), a função Γ, a fórmula Euler-Maclaurin, funções geradores e a fórmula produto para a função ζ.

Geometria

A maior parte do trabalho de Euler na área de geometria envolveu aplicações do cálculo a problemas geométricos. Como já mencionamos, foi muito ativo no desenvolvimento da geometria diferencial e, de fato, é considerado como um dos fundadores dessa subárea da matemática, sendo Gaspard Monge

(1746-1818) e C. F. Gauss (1777-1855) os outros dois. Homer S. White (2007) explica que o matemático suíço ainda fez extensivos estudos sobre a trigonometria esférica, classificou curvas planares do segundo grau, iniciou a classificação das curvas do terceiro grau e foi o primeiro a reconhecer a importância de geodésicas.

Dois dos seus trabalhos são considerados precursores da topologia. De fato, Leibniz havia concebido uma nova parte da matemática, que chamou de *analysis situs*, ou seja, análise da posição, em que certos problemas geométricos seriam abordados sem o recurso a conceitos métricos. Quando Euler conheceu o famoso problema das pontes de Königsbergo, ele o enquadrou nesse novo tipo de análise. Königsbergo, na época uma importante cidade da Prússia, é situado no Rio Pregel, o que divide a cidade em quatro setores (ver a Figura 6), sendo um desses setores uma ilha no meio do rio. Os setores foram ligados por sete pontes e daí nasceu o seguinte problema: será possível passear na cidade de tal forma a atravessar cada ponte uma única vez? Ainda mais, será possível terminar o passeio no ponto inicial?

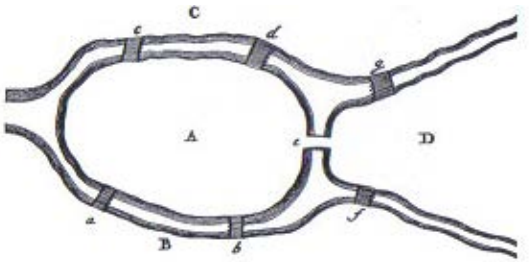

Figura 6. O diagrama de Euler para o problema de Königsbergo.
Fonte: *Apud* Hopkins e Wilson (2007).

Euler mostrou que o passeio procurado não existe no caso da configuração de Königsbergo, formulou e resolveu a versão generalizada do problema e deu um exemplo de uma configuração (ver a Figura 7) com duas ilhas (seis setores), quatro rios e quinze pontes, em que é possível fazer o passeio.

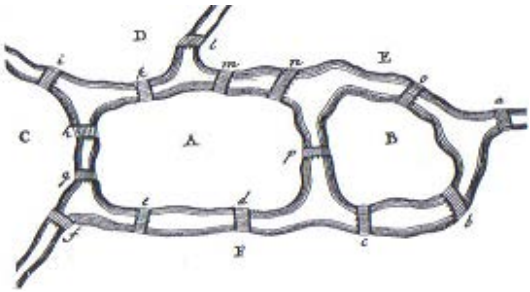

Figura 6. O diagrama de Euler para um problema com 15 pontes.
Fonte: *Apud* Hopkins e Wilson (2007).

O segundo dos referidos trabalhos sobre conceitos topológicos aborda o que hoje chamaríamos uma constante

topológica, a saber, F–E+V = 2, para certos tipos de poliedros, onde F é o número de faces do poliedro, E o número de arestas e V o número de vértices. Tentou demonstrar o teorema por reduzir o poliedro a um que é mais simples, fazendo a redução de tal maneira que a quantidade F–E+V permanece constante e, embora a sua demonstração acabasse tendo falhas, o teorema foi reformulado de maneira mias preciso e demonstrado por matemáticos posteriores.

Álgebra

A maior parte do trabalho de Euler na Álgebra foi na teoria de equações, desenvolvendo métodos para fatorar equações ou para achar raízes. Foi d'Alembert que deu certo impulso ao que depois seria chamado o teorema fundamental de álgebra, a saber, que um polinômio de grau *n* tem *n* raízes (complexas). Ele se interessava em achar integrais de quocientes de polinômios, o que seria facilitado se poderia fatorar o polinômio denominador em fatores lineares e/ou quadráticos. Neste contexto, o teorema tomou a seguinte forma: Todo polinômio com coeficientes reais pode ser decomposto em um produto de fatores lineares e/ou quadráticos. (A necessidade de trabalhar no campo dos números complexos para demonstrar esse teorema só seria compreendida mais tarde.)

Ao tentar demonstrar essa proposição, Euler foi, é claro, fadado a fracassar, pois não é universalmente válida. Mesmo assim, teve sucesso parcial, pois a mostrou para os casos em que $n = 4, 5$. Para o caso $n = 4$, fez uma substituição que eliminaria o termo cúbico. No caso em que o termo x é ausente, a solução é bastante fácil, pois a equação é uma quadrática em x^2 e pode ser resolvido diretamente, se o descriminante for positivo, ou transformado em uma diferença de dois quadrados, se o descriminante for negativo.

Quando o termo linear, x, não desaparece, no entanto, Euler conseguiu relacionar as raízes da equação por um sistema de equações e, consequentemente, expressá-las por uma só variável. Isto o levou a uma equação de grau 6 que poderia tratar como uma cúbica para achar as raízes. Para, garantir que as mesmas fossem reais, no entanto, ainda precisava invocar o teorema do valor intermediária do Cálculo. O mesmo teorema lhe permitiu reduzir equações de grau 5 a equações de grau 4 e, portanto, garantir que são faturáveis.

Ainda tentou aplicar a mesma estratégia a casos superiores, mas fez algumas suposições sobre a existência de raízes reais que invalidaram o resultado. Mesmo assim, como William Dunham (2007) observou, a virtuosidade com que lidou com as propriedades algébricas e as propriedades analíticas de

polinômios foi impressionante, mesmo levando em conta que só obteve resultados parciais.

Teoria dos Números

Como já indicamos, Euler, tendo escrito quase cem trabalhos sobre o assunto, fez vários contribuições à Teoria de Números. Esse ramo da matemática foi investigado por Fermat, mas a maioria dos seus contemporâneos pensava que era apenas uma coleção de problemas independentes e não uma verdadeira ciência e, portanto, mostrou pouco interesse no assunto. Mesmo assim, os Bernoulli abordavam alguns tópicos da Teoria dos Números e é provável que Euler tomou conhecimento desses tópicos através deles. Também tomou conhecimento do trabalho (em geral, conjeturas e desafios) de Fermat através da sua correspondência com Goldbach.

Além dos problemas originários de Fermat, Euler investigou as propriedades de números primos, questões relacionadas à divisibilidade e equações diofantinas. Foi pioneiro na aplicação de métodos algébricos à Teoria dos Números e desenvolveu novos conceitos, alguns dos quais foram precursores da Teoria dos Grupos. De modo geral, sua abordagem organizou e sistematizou o estudo dessa subárea da matemática de tal forma que foi reconhecida, para a primeira

vez, como uma parte legítima da ciência. Visto que suas contribuições particulares sobre a Teoria dos Números serão objeto de análise de outros volumes do presente *Arquivo*, não será necessário nos delongar sobre isto agora. Assim, voltamos a nossa atenção agora para o conteúdo do *Tratado* traduzido no Presente

Parte 3

Resumo do Conteúdo do *Tratado*

O *Tratado* foi provavelmente elaborado, segundo Weil (2001, p. 177), por volta de 1750, embora não tenha sido concluído. Assim, o texto que temos, publicado postumamente em 1849, deve ser concebido como uma primeira versão e não uma obra devidamente lapidada pelo seu autor. Mesmo assim, contém muito material interessante, além de, também, retratar as fronteiras da Teoria dos Números da época.

O primeiro capítulo, intitulado "Sobre a composição dos números," consiste de 54 parágrafos, começando com a definição pitagórica de *número*. A mesma também se encontra em *Os Elementos* de Euclides (Definição 2, Livro VII) e reza, na tradução de Irineu Bicudo (Euclides, 2009): "E número é quantidade composta de unidades." A ideia básica é que o conceito de número compreende o de quantidade, de tal forma que a sua multiplicidade é indicada pelas suas unidades componentes. Esses componentes, no entanto, são colecionados como uma unidade maior pela mente e o resultado é reificado para mais facilmente padecer as operações aritméticas. Ao mesmo tempo, Euler chama atenção a outro aspeto dos números, o de que cada um tem um determinado lugar na sequência

numérica que se desenvolve pela adjunção sucessiva de unidades. Aos números naturais (1, 2, 3, ...), acrescenta logo o zero, o que, contudo, é convenientemente esquecido na sua classificação posterior dos números em várias categorias. Isto se explique se entendermos o símbolo 0 a não representar um numeral, mas simplesmente o conceito *nada*, que é, aliás, o significado literal da palavra latina (*nihil*) usada por Euler – embora isto não seja inteiramente natural quando 0 é usado, por exemplo, em equações. Números negativos não são mencionados explicitamente no presente capítulo.

Adição e subtração são definidas pela junção e remoção de unidades. Multiplicação, como uma operação, não é abordada explicitamente, mas através do conceito de *múltiplo*, que, por sua vez, é definido recursivamente como a soma de parcelas iguais. Euler então afirma a comutatividade de multiplicação por observar que *ab* pode ser compreendido como contendo *a* parcelas de *b* ou *b* parcelas de *a*. Nenhum outro exemplo de que hoje consideraríamos axiomas para os inteiros (axiomas para anéis) é abordado. Na sua explicação de múltiplos, Euler deixa claro que *múltiplo* é equivalente ao *número composto* (embora ele não seja completamente consistente nisto); os não múltiplos, ou números *símplices*, são os *números primos*, entre os quais a unidade é incluída (e, novamente, excluída quando

conveniente)[1]. Devemos distinguir entre os símplices e o número *simples*, que é o menor termo positivo de uma classe de múltiplos. Por exemplo, 4 é o simples dos múltiplos de 4, embora 4 claramente não é primo.

Visto que todo produto pode ser quebrado em fatores menores até chegamos ao ponto em que não há mais qualquer fator composto, todo produto pode ser expresso como produto de números primos. Desta maneira, todos os números pertencem a classes disjuntas dependendo de quantos fatores primos (não necessariamente distintos) possuem. O capítulo fecha com algumas considerações sobre a distribuição nos números nessas classes, dando certa ênfase à distribuição irregular dos primos.

Os 27 parágrafos do segundo capítulo, "Sobre divisores de números," se iniciam com as definições de *divisor* e *quociente*. Mais uma vez, as definições são feitas com referência ao conceito de múltiplos; não obstante, suas definições são basicamente equivalentes à definição usada hoje em dia para "a divide b" ($a \mid b$). Em seguida, mostra que $1 \mid n$ e $n \mid n$, sempre que n é inteiro positivo. A prova, porém, é estranha, pois encara n como múltiplo de 1, embora já havia removido os números simples do conceito de múltiplos. Isto é concertado no §60, onde

[1] De fato, Euler, no próximo capítulo (§62), alegará que a unidade geralmente não é considerada primo porque estes têm dois divisores (positivos), enquanto a unidade tem apenas um.

prova que "$d \mid n \Rightarrow n$ é múltiplo de d," pois explicitamente alarga o conceito de múltiplo de novo para fazer a demonstração. Esse procedimento é típico do texto de Euler, pois ele alarga ou restringe o significado de vários conceitos, dependendo da conveniência do momento; às vezes, faz isto explicitamente e, às vezes, conta com o bom senso do leitor. Continuando, considere os números como pertencentes às classes definidas no capítulo anterior e define os *tipos* dos seus divisores através da sua decomposição em números primos. O final do capítulo (§73 a §91) é dedicado à demonstração da fórmula que determina o número de divisores de um número, isto é, para $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, onde p_1, p_2, ..., p_k são primos distintos e α_1 ,α_2, ..., α_k são números naturais, n tem $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)$ divisores, isto é, a referida fórmula define uma função multiplicativa. A demonstração é por "indução," ou seja, alguns casos especiais são mostrados e isto é considerado suficiente para estabelecer um padrão que pode ser generalizado; ou talvez melhor, espera-se que os casos mostrados sejam suficientes a levar o leitor a compreender como qualquer outro caso seria tratado.

O terceiro capítulo, "Sobre a soma dos divisores de qualquer número," contém 29 parágrafos dedicados a mostrar que, para p primo, a soma dos divisores de p^k é $p^k+p^{k-1}+\ldots+p+1$

$= \frac{p^{k+1}-1}{p-1}$ e que a soma dos divisores (indicada pelo símbolo $\int n$) é uma função multiplicativa. Lista as somas para várias classes e tipos de números e calcula $\int n$ para $1 \leq n \leq 60$. Observa que há números que não são somas de divisores de qualquer número, listando os mesmos para $n \leq 60$. Define um número perfeito como sendo um número N para o qual $\int N = 2N$, que é a definição moderna (a antiga, e equivalente, é que N = soma das suas partes alíquotas). Mostra que todo número perfeito par tem a forma $2^n(2^{n+1}-1)$, com $2^{n+1}-1$ primo (ver *Os Elementos* de Euclides, Proposição 36 de Livro IX). Observa ainda que ninguém sabe se há números primos ímpares, mas que, se houver, terão a forma $(4n+1)^{4\lambda+1}P^2$, onde P é um número ímpar e $4n+1$ é primo.

O quarto capítulo, "Sobre números primos e compostos entre si," consiste de 29 parágrafos. Inicia-se por definir números *primos entre si* e, em paralelo, números *compostos entre si*. A maior parte do capítulo, no entanto, investiga, para um dado número n, a questão da quantidade de números contidos no intervalo de 1 a n que são primos com n. Hoje, isto é geralmente chamado a função φ de Euler, embora ele não usa essa notação na presente obra. Mostra que $\varphi(p^n) = p^{n-1}(p-1)$ para p primo e mostra que φ é uma função multiplicativa. Nesse capítulo achamos, pela primeira vez, a transcrição de algumas

anotações que Euler fez na margem do seu texto. Nela enuncia as seguintes proposições[2]:

- Sejam a e b números primos e c um número qualquer. Então, $\exists n, q$, tais que $na = bq+c$.
- $(a, b) = 1 \Rightarrow (a^{\alpha}, b^{\beta}) = 1$.
- $(a, b) = 1$ e $(a, c) = 1 \Rightarrow (a, bc) = 1$.
- Para p primo, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.
- $(a, b) = 1 \Rightarrow$ para qualquer k, $\exists m, n$, tais que $ma–nb = 1$ e, portanto, $\exists m', n'$, tais que $m'a–n'b = k$.
- $(a, b) = d \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
- $a = bq+r \Rightarrow na = nbq+nr$.
- $a = bq+r$, $c \mid a$ e $c \mid b \Rightarrow c \mid r$.
- $a = bq+r$, $c \mid b$ e $c \mid r \Rightarrow c \mid a$.
- O Algoritmo de Euclides (aplicado aos números a, b tais que $(a, b) = 1$).

Várias dessas proposições são importantes por si só; parece, contudo, que o propósito de Euler foi o de demonstrar o Algoritmo de Euclides para achar o M.D.C.

No próximo capítulo, o quinto, intitulado "Sobre resíduos surgidos por divisão," Euler inicia seu estudo de resíduos. Nos 27 parágrafos do capítulo, utiliza o Algoritmo da

[2] Aqui (a, b) significa o M.D.C. entre a e b. Assim, $(a, b) = 1$ indica que a e b são primos entre si. Observe também que não é inteiramente claro do texto de Euler se os expoentes α e β da segunda proposição devem ser concebidos como sendo, possivelmente, distintos ou se, para ele, devem ser iguais. Assim, damos a interpretação mais geral.

Divisão para definir "resíduo" e aborda a aritmética elementar dos mesmos, mostrando que o resíduo da soma, diferença e produto de dois números correspondam à soma, diferença e produto dos resíduos dos números originais. É evidente que está investigando o que hoje chamamos "congruência módulo *m*", pois afirma que dado um divisor qualquer *d*, os inteiros (explicitamente inclui os negativos) são divididos em *d* classes, sendo que todos os elementos de uma mesma classe são equivalentes; também substitui livremente números pelos seus equivalentes. Não possui, contudo, a notação sugestiva que seria desenvolvida mais tarde por Gauss e, portanto, desenvolve suas considerações ou retoricamente ou através das fórmulas ($nd+r$) que geram as classes.

O sexto capítulo, "Sobre resíduos surgidos da divisão de termos em progressão aritmética," contém 25 parágrafos em que se investiga os resíduos dos termos de progressões aritméticas. Há dois casos diferentes. No primeiro, a diferença comum (b) é primo com o divisor (d). Euler mostra que, nesse caso, todos os números de 0 a d–1 são resíduos. No segundo caso, $(b, d) = f > 1$ e há D resíduos distintos, onde $d = Df$. Além disto, todos os resíduos serão a soma de a, o primeiro termo da progressão, com algum múltiplo do M.D.C. (f). Observamos que, formalmente, o primeiro caso pode ser incluído no segundo por permitir que $f = 1$.

Assim, teríamos $d = D \times 1$. No entanto, a formulação do texto é provavelmente mais perspícua. Em todos os dois casos, a sequência dos d, ou D, resíduos se repete ciclicamente.

Euler passa a investigar os resíduos dos termos em progressões geométricas nos 51 parágrafos do sétimo capítulo, que é intitulado "Sobre resíduos surgidos da divisão de termos em progressão geométrica." Mostra que a investigação pode ser reduzida ao caso em que o termo inicial é a unidade e o fator comum (b) é primo com o divisor (d). Nestas condições, mostra o Teorema de Euler, $b^{\varphi(d)} \equiv 1 \pmod{d}$ se a e d são coprimos e φ é a função de Euler, embora, como já mencionamos, não usa a linguagem de congruência; também mostra, como consequência, uma versão do Pequeno Teorema de Fermat. Finaliza o capítulo por mostrar que se $b^n \equiv 1 \pmod{d}$ com $0 < n \leq \varphi(d)$, então $n \mid \varphi(d)$.

No oitavo capítulo, intitulado "Sobre potências de números que, quando divididos por números primos, deixam a unidade," que consiste de 21 parágrafos, Euler investiga $a^n \equiv 1 \pmod{d}$ para d primo ímpar e, portanto, da forma $2p+1$. A discussão é feita em termos da divisibilidade de a^n-1 por d. Mostra primeiro que $a^n \equiv 1 \pmod{d}$ e $(n, 2p) = \lambda$ implica que $a^\lambda \equiv 1 \pmod{d}$ e, em seguida, que, para n primo, os divisores primos de a^n-1, que não são divisores de $a-1$, são contidas na

forma $2mn+1$. Finaliza o capítulo mostrando que, para todo primo da forma $d = 2p+1$, sempre há algum a tal que a^n não é congruente à unidade módulo d.

Nos 20 parágrafos do nono capítulo, "Sobre divisores de números da forma $a^n \pm b^n$," Euler, em primeiro lugar, pergunta quais números primos ímpares, $2p+1$, além dos divisores de $a-b$ dividem a^n-b^n. Particularizando um resultado mais geral, deduz que, para n primo e $(a, b) = 1$, os divisores primos de a^n-b^n têm a forma $\lambda n+1$. De forma semelhante, se n é o produto de dois primos, α e β, os referidos divisores são os que têm as formas $\lambda\alpha+1$, sendo $(\lambda, \beta) = 1$, $\lambda\beta+1$, sendo $(\lambda, \alpha) = 1$, e $\lambda\alpha\beta+1$. Então, mostra que primos da forma $\lambda\alpha+1$ não dividem $a^\beta-b^\beta$. Assim, fazendo $n = 2m$, usa a fórmula $a^{2m}+b^{2m} = (a^m-b^m)(a^m+b^m)$ para deduzir que os divisores de a^m+b^m tem a forma $2\lambda m+1$.

Euler investiga os resíduos de quadrados perfeitos no décimo capítulo, intitulado "Sobre resíduos surgidos da divisão de quadrados por números primos." O referido capítulo, consistindo de 87 parágrafos, é o maior do livro. Euler considera divisores primos maiores que 2 e, assim, põe $d = 2p+1$. Neste caso, mostra que há exatamente p resíduos e p não-resíduos entre os números de 1 a $2p$. Prossegue mostrando que (*i*.) o produto de dois resíduos é um resíduo (e, portanto, qualquer potência de um resíduo é um resíduo, o que lhe permite a

comparar os resíduos quadráticos com os resíduos surgidos de sequências geométricas, estudados em Capítulos VII e VIII), (*ii*.) o produto de um não-resíduo e um resíduo é um não-resíduo e (*iii*.) o produto de dois não-resíduos é um resíduo. Então, define o "complemento" de um número r menor que d como o número c tal que $r+c = d$ e mostra que, quando $d = 4q+1$, os complementos de resíduos são resíduos e, quando $d = 4q-1$, os complementos de resíduos são não-resíduos. Ao fazer isto, também mostra que o número primo $d = 4q+1$ pode ser representado como a soma de dois quadrados, primos entre si, e que isto não é o caso para $d = 4q-1$. Estabelece que, para $d = 2p+1$, primo, se a^p-1 é divisível por d, a é um resíduo e, se a^p+1 é divisível por d, a é um não-resíduo. Isto é conhecido hoje em dia como o *critério de Euler*. Ainda mostra que, quando $d = 4q+1$, achamos -1 entre os resíduos e, portanto, o simétrico de todo resíduo é um resíduo, enquanto, ao contrário, quando $d = 4q-1$, o número -1 é um não-resíduo. Observe o caso importante de que $+2$ é resíduo para $d = 4q+1$ e não-resíduo para $d = 4q-1$; faz ainda observações semelhantes para outros casos especiais. Com isto, Euler começa sua abordagem do que é hoje conhecido como "reciprocidade quadrática". Isso, no entanto, não é inteiramente óbvio, pois ele não se ocupa com o próprio conceito de reciprocidade (isto é, o de dois números

relacionados de tal forma que cada um é um resíduo do outro); sempre procura vários divisores de certas formas dos quais *n* é um resíduo e não dá, nem teoricamente, nem nos poucos exemplos numéricos, qualquer indício que está à procura da relação de reciprocidade. Assim, sua abordagem não tem a simplicidade e elegância de formulações posteriores como os de Legendre[3] e, sobretudo, Gauss. Mesmo assim, Edwards (2007) observa que o desenvolvimento desse material por autores mais modernos perdeu o aspecto explícito de reciprocidade e voltou a um ponto de vista mais de acordo com o de Euler, o que, sempre segundo o referido autor, atesta à genialidade do Euler. Em qualquer caso, observamos que Euler não conseguiu demonstrar muita coisa referente à questão de reciprocidade, mas apresentou vários "teoremas" – isto é, para nós, conjecturas – baseadas em exemplos concretos. Assim, pode-se perguntar se Euler teve alguma influência importante no desenvolvimento posterior do assunto. Weil, (2001, p. 210), comentando sobre Capítulos 10 a 12 do *Tractatus*, emite o seguinte julgamento:

> These brilliant but wholly isolated observations were lost to the mathematical world; in 1849, when the *Tractatus* was first published, Gauss, and then Jacobi and Eisenstein, had already proved all that Euler had guessed, and of course much more.

[3] Legendre deu sua primeira versão desta lei em 1785. Posteriormente, deu outras versões. A obra mais acessível dele sobre a Teoria dos Números é Legendre (1830).

Devemos lembrar, porém, que Euler cientificou sua abordagem do tópico a outros matemáticos da época através da sua correspondência e apresentou a mesma à Academia de São Petersburgo em 1748 como "Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum," que foi publicado em 1751. De fato, Euler é geralmente considerado como um dos principais incentivadores de pesquisa sobre reciprocidade da sua época.

No décimo primeiro capítulo, "Sobre resíduos surgidos da divisão de cubos por números primos", que consiste de 41 parágrafos, Euler empreende um estudo sobre os resíduos deixados por cubos perfeitos. Observe que se a^3 deixar o resíduo r, o cubo do complemento da sua raiz, $(d-a)^3$, deixará o resíduo $-r$. Observa ainda que quando o divisor primo tiver a forma $6q+1$, um terço dos números de 1 a $6q$ serão resíduos, sendo o restante não-resíduos; senão, os $6q$ resíduos serão distintos. Mostra que a multiplicação de resíduos e não-resíduos é parecida com o que aconteceu para resíduos quadráticos, exceto no caso do produto de dois não-resíduos, que pode ser tanto resíduo, quanto não-resíduo. Ainda separa os não-resíduos em duas classes equinumerosas, obtidas de um não-resíduo A, multiplicando cada resíduo primeiro por A e, depois, por A^2; desta forma, o produto de dois não-resíduos da mesma classe

resulta em um não-resíduo da outra classe, enquanto o produto de dois resíduos de classes diferentes resulta em um resíduo. Afirma que se o primo $d = 6q+1$ dividir $p^3 \pm aq^3$, então a será um resíduo para o referido divisor. Conjectura ainda certas condições para 2, 3, 5, 6, 7 e 10. Nos primeiros quatro casos, dá vários exemplos e será interessante especificar os cálculos para esses exemplos.

Para 2 ser resíduo, então, Euler afirma que o divisor primo d, da forma $6q+1$, também deve ser da forma $27p^2+q^2$. As representações, na forma indicada, dos exemplos dados por Euler são os seguintes:

$31 = 27(1)^2+ 2^2$ $\quad$ $499 = 27(3)^2+16^2$
$43 = 27(1)^2+ 4^2$ $\quad$ $601 = 27(4)^2+13^2$
$109 = 27(2)^2+ 1^2$ $\quad$ $643 = 27(3)^2+20^2$
$127 = 27(1)^2+10^2$ $\quad$ $691 = 27(5)^2+ 4^2$
$157 = 27(2)^2+ 7^2$ $\quad$ $727 = 27(3)^2+22^2$
$223 = 27(1)^2+14^2$ $\quad$ $733 = 27(2)^2+25^2$
$229 = 27(2)^2+11^2$ $\quad$ $739 = 27(5)^2+ 8^2$
$277 = 27(2)^2+13^2$ $\quad$ $811 = 27(1)^2+28^2$
$283 = 27(1)^2+16^2$ $\quad$ $919 = 27(3)^2+26^2$
$307 = 27(3)^2+ 8^2$ $\quad$ $997 = 27(6)^2+ 5^2$
$397 = 27(2)^2+17^2$ $\quad$ $1021 = 27(6)^2+ 7^2$
$433 = 27(4)^2+ 1^2$ $\quad$ $1051 = 27(1)^2+32^2$
$439 = 27(3)^2+14^2$ $\quad$ $1069 = 27(2)^2+31^2$
$457 = 27(4)^2+ 5^2$ $\quad$ $1093 = 27(6)^2+11^2$

Para 3 ser resíduo, temos $d = 3p^2+q^2$ com $p = 9n$ ou $p\pm q = 9n$:

$$\begin{aligned}
61 &= 3(2)^2+ 7^2 \quad \text{onde} \quad 2+7 = 9(1)\\
67 &= 3(1)^2+ 8^2 \quad \text{onde} \quad 1+8 = 9(1)\\
73 &= 3(4)^2+ 5^2 \quad \text{onde} \quad 4+5 = 9(1)\\
103 &= 3(1)^2+10^2 \quad \text{onde} \quad 1-10 = 9(-1)\\
193 &= 3(8)^2+ 1^2 \quad \text{onde} \quad 8+1 = 9(1)\\
307 &= 3(9)^2+ 8^2 \quad \text{onde} \quad 9 = 9(1)\\
367 &= 3(11)^2+2^2 \quad \text{onde} \quad 11-2 = 9(1)\\
439 &= 3(9)^2+14^2 \quad \text{onde} \quad 9 = 9(1)\\
577 &= 3(4)^2+23^2 \quad \text{onde} \quad 4+23 = 9(3)\\
1021 &= 3(18)^2+7^2 \quad \text{onde} \quad 18 = 9(2)
\end{aligned}$$

Para 5 ser resíduo, temos $d = 3p^2+q^2$ com (*i*.) $p = 15n$, (*ii*.) $p = 3m$ e $q = 5n$, (*iii*.) $p\pm q = 15n$, ou (*iv*.) $p\pm 2q = 15n$:

$$\begin{aligned}
13 &= 3(2)^2+ 1^2 \quad \text{onde} \quad 2-2(1) = 15(0) \quad \text{Cond. } (iv.)\\
67 &= 3(1)^2+ 8^2 \quad \text{onde} \quad 2-2(8) = 15(-1) \quad \text{Cond. } (iv.)\\
127 &= 3(3)^2+10^2 \quad \text{onde } 3 = 3(1) \text{ e } 10 = 5(2) \quad \text{Cond. } (ii.)\\
181 &= 3(2)^2+13^2 \quad \text{onde} \quad 2+13 = 15(1) \quad \text{Cond. } (iii.)\\
199 &= 3(1)^2+14^2 \quad \text{onde} \quad 1+14 = 15(1) \quad \text{Cond. } (iii.)\\
241 &= 3(8)^2+ 7^2 \quad \text{onde} \quad 8+7 = 15(1) \quad \text{Cond. } (iii.)\\
487 &= 3(1)^2+22^2 \quad \text{onde } 1+44 = 15(3) \quad \text{Cond. } (iv.)\\
739 &= 3(15)^2+ 8^2 \quad \text{onde} \quad 15 = 15(1) \quad \text{Cond. } (i.)
\end{aligned}$$

Finalmente, para 6 ser resíduo, temos $d = 3p^2+q^2$ com $p = 9n$ ou $2p\pm q = 9n$:

$$\begin{aligned}
7 &= 3(1)^2+ 2^2 \quad \text{onde} \quad 2(1)-2 = 9(0)\\
37 &= 3(2)^2+ 5^2 \quad \text{onde} \quad 2(2)+5 = 9(1)\\
139 &= 3(5)^2+ 8^2 \quad \text{onde} \quad 2(5)+8 = 9(2)\\
163 &= 3(7)^2+ 4^2 \quad \text{onde} \quad 2(7)+4 = 9(2)
\end{aligned}$$

$$
\begin{aligned}
181 &= 3(2)^2+13^2 \quad \text{onde} \quad 2(2)-13 = 9(-1)\\
241 &= 3(8)^2+\ 7^2 \quad \text{onde} \quad 2(8)-7 = 9(1)\\
307 &= 3(9)^2+\ 8^2 \quad \text{onde} \quad 9 = 9(1)\\
337 &= 3(4)^2+17^2 \quad \text{onde} \quad 2(4)-17 = 9(-1)\\
349 &= 3(10)^2+7^2 \quad \text{onde} \quad 2(10)+7 = 9(3)\\
379 &= 3(11)^2+4^2 \quad \text{onde} \quad 2(11)-4 = 9(2)\\
631 &= 3(7)^2+22^2 \quad \text{onde} \quad 2(7)+22 = 9(4)\\
727 &= 3(9)^2+22^2 \quad \text{onde} \quad 9 = 9(1)\\
751 &= 3(5)^2+26^2 \quad \text{onde} \quad 2(5)+26 = 9(4)\\
997 &= 3(18)^2+5^2 \quad \text{onde} \quad 18 = 9(2)
\end{aligned}
$$

Com a possível exceção do primeiro caso, as condições são bastante complexas para a quantidade de instâncias usadas para fazer a generalização. De fato, para o caso do resíduo 5, nenhum exemplo da condição $p-q = 15n$ é dado.[4] Isto poderá indicar, se acatarmos a afirmação de Euler de que procedeu por "indução", que ele realmente investigou muito mais casos do que os que relatou no presente capítulo, ou que foi bastante afoito nas suas generalizações.

Nos 51 parágrafos do décimo segundo capítulo, intitulado "Sobre resíduos surgidos da divisão de biquadrados por números primos", Euler manifesta preocupações parecidas com as dos capítulos anteriores. Mostra que se o divisor primo tiver a forma de $4q-1$, haverá $2q-1$ resíduos distintos em relação

[4] Um exemplo seria $d = 769 = 3(16)^2+1^2$. Observe que o referido d é um primo da forma $6q+1$.

aos biquadrados e, caso contrário, se o divisor for da forma $4q+1$, haverá q resíduos distintos. No segundo caso, haverá ainda três classes de não-resíduos, cada uma contendo q elementos. Ainda elabora regras de pertinência para a multiplicação de elementos das várias classes, determina quais resíduos de quadrados são também resíduos de biquadrados e observa que números primos da referida forma sempre podem ser representados como a soma de dois quadrados. Finalmente, conjectura sob quais condições –2, 2, 3, –4, 5 e q são resíduos de biquadrados para os divisores primos da forma $4q+1$.

No décimo terceiro capítulo, "Sobre resíduos surgidos da divisão de surdosólidos por números primos," Euler dedica 39 parágrafos aos resíduos de números da forma x^5. O termo *surdo* foi usado para indicar uma raiz irracional de um inteiro ($\sqrt{2}$ ou $\sqrt[3]{2}$) ou uma combinação deles ($\sqrt{2}+\sqrt[3]{2}$), enquanto o termo *número sólido* indicava que o número tinha três fatores, ou seja, um cubo, caso os fatores fossem iguais. Assim, a combinação desses termos, isto é, *surdosólido*, ou (inapropriadamente) *sursólido*, indicava uma quinta potência.[5] Mostra que, quando o divisor primo não for da forma $10q+1$, haverá $10q$ resíduos distintos, enquanto que, se for da referida forma, haverá $2q$ resíduos distintos e $8q$ não-resíduos, sendo estes últimos

[5] Ver, por exemplo, Barlow (1814) ou Hutton (1796).

distribuídos em quatro classes diferentes. Assim, dado qualquer número a, menor que o divisor, terá mais quatro números, igualmente menores que o divisor, tais que tenham o mesmo resíduo que a. Euler então mostra que a soma desses cinco números sempre será divisível pelo divisor original $10q+1$ e generaliza alguns dos seus resultados para divisores primos da forma $mn+1$.

Nos 39 parágrafos do décimo quarto capítulo, "Sobre resíduos surgidos da divisão de quadrados por números compostos," investiga-se, em primeiro lugar, divisores compostos das formas $2(2p+1)$, $4(2p+1)$ e $8(2p+1)$, onde, como sempre, $2p+1$ é um primo ímpar. Para todos os três divisores, há p resíduos; a quantidade de não-resíduos, porém, é diferente para cada divisor, sendo, respectivamente, p, $3p$ e $7p$. Para cada caso, mostra a relação entre os resíduos do divisor $2p+1$ e os resíduos do divisor composto. No primeiro caso, por exemplo, os resíduos ímpares do divisor $2p+1$ são também divisores do divisor $2(2p+1)$, enquanto os resíduos pares do primeiro somados com o próprio $2p+1$ completam o conjunto de resíduos do divisor composto. Desta maneira, todos os resíduos do divisor $2(2p+1)$ são números ímpares. Euler ainda fecha o capítulo com algumas rápidas considerações sobre os resíduos dos divisores $3(2p+1)$ e $(2p+1)(2q+1)$, onde, no primeiro caso,

$2p+1$ é um número primo maior que 2 e, no segundo, $2p+1$ e $2q+1$ são primos distintos. Ele dá destaque à afirmação (as demonstrações são incompletas) de que há p resíduos distintos no primeiro caso e pq deles no segundo.

No décimo quinto capítulo, consistindo de 30 parágrafos e intitulado "Sobre os divisores de números da forma $xx+yy$," o resultado principal é que todo número primo da forma $4q+1$ pode ser representado como uma soma de dois quadrados, a^2+b^2, onde a e b são primos entre si. Em contraste, nenhum número primo da forma $4q-1$ pode ser representado por uma soma do referido tipo. As regras para o produto e o quociente de números representáveis por somas de dois quadrados são estabelecidas e é deduzido, como consequência, que a soma de dois quadrados, primos entre si, não pode ser dividida por um número da forma $4q-1$.

Finalmente, o último capítulo, intitulado "Sobre os divisores de números da forma $xx+2yy$," investiga os divisores de números da forma x^2+2y^2, onde x e y são primos entre si. Através de considerações sobre a paridade de x e y, determina que qualquer número desse tipo terá a forma $8n+1$, $8n+3$, ou o duplo destes. Ainda afirma que o produto e o quociente (quando existe) de dois números do referido tipo são do mesmo tipo. O capítulo contém apenas 17 parágrafos e é bastante provável que

Euler, se tivesse concluído a obra, teria acrescentado algumas considerações sobre o caso geral x^2+ny^2. Weil (2001) mostra que Euler não percebeu certas relações provenientes da Teoria dos Grupos e, portanto, o *Tratado* foi prematuro e tinha de ser abandonado. Isto, claro, é um juízo feito a partir de desenvolvimentos que ainda aconteceriam (o que não o invalida) Mas, do ponto de vista do próprio Euler, os últimos capítulos deveriam ter parecidos aquém da clareza e beleza dos capítulos iniciais – ele mesmo achou problemas com algumas demonstrações e a existência das suas notas nas margens indica (em contraste às famosas notas marginais de Pascal) a sua intenção de reformular o manuscrito. Não sabemos por que isto não foi feito, embora vários assuntos[6] lançados no presente manuscrito foram desenvolvidos em outros trabalhos seus.

Sobre a Tradução

Embora o latim fosse a linguagem culta dos cientistas europeus da época de Euler, é, mesmo assim, essencialmente uma língua antiga e carece dos recursos, especialmente no que se diz referente ao vocabulário, que o faria um instrumento ideal para expressar as subtilezas da matemática moderna. O problema é exacerbado pelo fato de que Euler estava investigando território novo, para o qual uma terminologia

[6] Para uma listagem desses assuntos, ver Weil (2001, p. 195ff).

padrão ainda não havia sido determinada e pelo fato de que ele foi, de certa forma, parcimonioso com o uso do formalismo algébrico. A presente tradução não tenta reproduzir esses aspectos do texto original, mas pretende apresentar ao leitor o pensamento de Euler sem, por um lado, se perder em questões linguísticas, nem, por outro lado, recorrer às falsas modernizações do texto original. Para tanto, incluímos algumas notas explicativas que poderão ajudar na interpretação do texto por esclarecer textos ambíguos, preencher lacunas no argumento, ou fazer referências internas às várias partes relevantes do texto. São todas incluídas como notas de rodapé e identificadas pela abreviação "N. do Trad." (Nota do Tradutor). As notas do próprio Euler, escritos à mão nas margens do seu manuscrito, foram colocadas na rodapé na publicação original (*Commentationes arithmeticae*, editado por P. H. Fuss e Nicolaus Fuss, 1849) e identificadas por uma frase em itálico da autoria dos editores. Aqui, são colocadas no texto imediatamente após o parágrafo em que aparecem, identificadas pelo sinal (*) e pela manutenção (em itálico) da frase explicativa dos referidos editores.

Identificamos vários erros no decorrer do texto. A maioria deles parecem ser erros de composição gráfica. Assim, corrigimos esses erros na tradução, mas sempre acrescentamos uma nota de rodapé identificando a correção e dando o texto original.

Referências

BARBEAU, E. J. Euler Subdues a Very Obstreperous Series. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 135-146.] Washington, DC: MAA, 2007.

BARLOW, Peter. *A New Mathematical and Philosophical Dictionary*. London: G. & S. Robinson, 1814.

BELL, E. T. *Men of Mathematics*. New York: Simon & Schuster, 1937.

BREIDERT, Wolfgang. Leonhard Euler and Philosophy. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 97-108.] Amsterdam: Elsevier, 2007.

BROWN, B. H. The Euler-Diderot Anecdote. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 57-59.] Washington, DC: MAA, 2007.

CALINGER, Ronald S. Leonhard Euler: Life and Thought. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 5-60.] Amsterdam: Elsevier, 2007.

CONDORCET, *Eulogy to Mr. Euler*. 2005. [Originalmente, 1786.] Disponível em: <http://www.math.dartmouth.edu/~euler/>. Acesso em: 20/04/2010.

DAVIS, Philip J. Leonhard Euler's Integral: A Historical Profile of the Gamma Function. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 167-184.] Washington, DC: MAA, 2007.

DUNHAM, William. Euler and the Fundamental Theorem of Algebra. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 243-255.] Washington, DC: MAA, 2007.

EDWARDS, Harold M. Euler and Quadratic Reciprocity. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 233-242.] Washington, DC: MAA, 2007.

ECKERT, Michael. Euler and the Fountains of Sanssouci. *Archive for the History of the Exact Sciences*, v. 56, p. 451-468, 2002.

EUCLIDES. *Os Elementos*. Tradução de Irineu Bicudo. São Paulo: Editora da UNESP, 2009.

FASANELLI, Florence. Images of Euler. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 109-120.] Amsterdam: Elsevier, 2007.

FELLMANN, Emil. *Leonhard Euler*. Tradução de Erika Gautschi & Walter Gautschi. Basel: Birkhäuser Verlag, 2007.

FERZOLA, Anthony P. Euler and Differentials. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 155-165.] Washington, DC: MAA, 2007.

FINKEL, B. F. Leonhard Euler. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 5-12.] Washington, DC: MAA, 2007.

FUSS, Nicolas. *Eulogy of Leonhard Euler*. Tradução de John S. D. Glaus. 2005. Disponível em: <http://www.math.dartmouth.edu/~euler/>. Acesso em: 20/04/2010.

HOFFMANN, Peter. Leonhard Euler and Russia. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 61-73.] Amsterdam: Elsevier, 2007.

HOPKINS, Brian e WILSON, Robin. The Truth about Königsberg. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 409-420.] Amsterdam: Elsevier, 2007.

HUTTON, Charles. *A Mathematical and Philosophical Dictionary*. London: J. Johnson, 1796.

KATZ, Victor J. Euler's Analysis Textbooks. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 213-233.] Amsterdam: Elsevier, 2007.

KLINE, Morris. Euler and Infinite Series. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 101-111.] Washington, DC: MAA, 2007.

KOETSIER, Teun. Euler and Kinematics. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 167-194.] Amsterdam: Elsevier, 2007.

KREYSZIG, Erwin. On the Calculus of Variations and its Major Influences on the Mathematics of the First Half of our Century. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 209-214.] Washington, DC: MAA, 2007.

LANGTON, Stacy G. Euler on Rigid Bodies. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 195-211.] Amsterdam: Elsevier, 2007.

LEGENDRE Adrien-Marie. *Théorie des Nombres*. Paris: A. Blanchard, 1955. [Originalmente 1830.].

LÜTZEN, Jesper. Euler's Vision of a General Partial Differential Calculus for a Generalized Kind of Function. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 197-207.] Washington, DC: MAA, 2007.

O'CONNOR, J. J. e ROBERTSON, E.F. Euler Portraits. 2008. Disponível em <http://www-history.mcs.st-andrews.ac.uk/PictDisplay/Euler.html>. Acesso em: 22/05/2010.

_____. Nicolaus Fuss. 2006. Disponível em: <http://www-history.mcs.st-andrews.ac.uk/Biographies/Fuss.html>. Acesso em: 28/04/2010.

_____. Leonhard Euler. 1998. Disponível em: <http://www-history.mcs.st-andrews.ac.uk/Biographies/Euler.html>. Acesso em: 20/04/2010.

REICH, Karin. Euler's Contribution to Differential Geometry and its Reception. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 479-502.] Amsterdam: Elsevier, 2007.

SANDIFER, C. Edward. Some Facets of Euler's Work on Series. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 279-302.] Amsterdam: Elsevier, 2007.

THIELE, Rüdiger. Euler and the Calculus of Variations. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 235-254.] Amsterdam: Elsevier, 2007.

TRUESDELL, C. Leonard Euler, Supreme Geometer. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 13-41.] Washington, DC: MAA, 2007.

WEIL, André. Euler. *In*: William Dunham (Ed.). *The Genius of Euler: Reflections on his Life and Work*. [p. 43-49.] Washington, DC: MAA, 2007.

_____. *Number Theory: An approach through history from Hammurapi to Legendre*. Boston: Birkhäuser, 2001.

WHITE, Homer S. The Geometry of Leonhard Euler. *In*: Robert E. Bradley and C. Edward Sandifer (Ed.). *Leonhard Euler: Life Work and Legacy*. [p. 303-321.] Amsterdam: Elsevier, 2007.

WILSON, Robin. "Read Euler, read Euler, he is the master of us all." 2007. Disponível em <http://plus.maths.org/Issue42/features/wilson>. Acesso em: 20/04/2010.

_____.Euler. 2002. Disponível em: <http://www.gresham.ac.uk/event.asp?PageId=4&EventId=67>. Acesso em: 20/04/2010.

Tratado sobre a Teoria dos Números

em XVI Capítulos

Capítulo I

Sobre a composição dos números

1. *Número* é uma quantidade de unidades.

2. Qualquer número, portanto, significa tanto quanto há unidades nele contidas.

3. Os números, começando com a unidade, são 1, 2, 3, 4, 5, 6, *etc*., cada um dos quais supera o anterior por uma unidade.

4. Visto que cada número pode ser aumentado por uma unidade, a série dos números progride ao infinito.

5. Desde que o primeiro, a saber, a unidade, também supera o anterior por uma unidade, é necessário que o referido anterior seja nada, 0.

6. O presente tratado está voltado apenas para os números inteiros e é somente acerca dos mesmos que a definição se aplica; em consequência, as frações e, ainda mais, os surdos devem ser excluídos.

7. Seja a um número qualquer; então, os que seguem serão a+1, a+2, a+3, a+4, *etc*., dos quais o primeiro, a+1, supera o dado número a por uma unidade, o segundo, a+2, por duas unidades, o terceiro, a+3, por três unidades, *etc*.

8. Semelhantemente, para o número proposto *a*, os anteriores serão *a*–1, *a*–2, *a*–3, *a*–4, *etc*., dos quais o primeiro, *a*–1, é menor que o dado número *a* por uma unidade, o segundo, *a*–2, por duas unidades, o terceiro, *a*–3 por três e, assim, sucessivamente.

9. Sejam juntadas ao número *a* tantas unidades quantas o número *b* contém; então, teremos *a*+*b*. Sejam, ao contrário, retiradas de *a* tantas unidades quantas *b* contém; então, teremos *a*–*b*. No primeiro caso, dizemos que o número *b* é *somado* ao número *a* e, no segundo, que é *subtraído* de *a*.

10. Seja o número *a* juntado a si mesmo; então teremos seu duplo *a*+*a*, que é escrito 2*a*. Seja o mesmo somado mais uma vez; então o triplo 3*a* será produzido. Se o mesmo número *a* for juntado mais uma vez, teremos seu quádruplo 4*a*, e assim sucessivamente. Estes são chamados, de modo genérico, *múltiplos* de *a*.

11. Os múltiplos de *a*, portanto, são 2*a*, 3*a*, 4*a*, 5*a*, *etc*, dos quais cada um supera o anterior pelo próprio número *a*; com respeito a estes, o próprio número *a* é chamado *simples*.

12. Se *a* for a unidade, todos os números serão claramente seus múltiplos; e se *a* não for a unidade, mas uma quantidade de unidades, nem todos os números serão seus múltiplos – neste caso, haverá números que não são múltiplos de *a*.

13. Visto que os múltiplos do próprio *a* são 2*a*, 3*a*, 4*a*, 5*a*, *etc*., todos os números menores que *a*, isto é, 1, 2, 3, ..., (*a*–

1), não se encontram entre esses múltiplos; e a mesma quantidade de não-múltiplos ocorrem entre qualquer múltiplo e o próximo.

14. Se, portanto, α for um número menor que a, nem α nem os números $a+\alpha$, $2a+\alpha$, $3a+\alpha$, $4a+\alpha$, *etc*. se encontram entre os múltiplos de a.

15. Visto que, para $\alpha < a$, $2a-\alpha$ é menor que $2a$ e, ao mesmo tempo, maior que a, o número $2a-\alpha$ não será um múltiplo do a; também nenhum dos números $a-\alpha$, $2a-\alpha$, $3a-\alpha$, $4a-\alpha$, *etc*. será contido entre os múltiplos de a.

16. Dado, portanto, um número b qualquer, que não seja um múltiplo de a, ele será ou menor que a, ou superará um certo múltiplo do mesmo, sendo, contudo, menor que o próximo múltiplo.

17. Visto que os múltiplos de dois (dos quais não excluo o número simples) são 2, 4, 6, 8, 10, *etc*., os outros números diferem destes por uma unidade. De forma semelhante, em relação aos múltiplos de três, 3, 6, 9, 12, 15, *etc*., os outros números distam desses, ou por uma unidade, ou por duas.

18. O dobro de um número a qualquer, isto é $2a$, é também um múltiplo de dois. Mas, como a é uma quantidade de unidades 1+1+1+1 *etc*., seu redobramento poderia ser representado da seguinte maneira:

$$a = 1+1+1+1+etc.$$

$$a = 1+1+1+1+etc.$$

que, somando, resulta em $2a = 2+2+2+2+etc.$

19. Ou seja, visto que o número a é uma quantidade de unidades, o número a será dobrado ao tomar cada unidade duas vezes, o que faz surgir uma quantidade de binários. Disto, é claro que o duplo $2a$ contém tantos binários, quantas unidades são contidas em a.

20. Do mesmo modo, o triplo $3a$ conterá tantos trios, quantas unidades são contidas em a e, portanto, $3a$ também será um múltiplo de 3. O mesmo deve ser entendido sobre todos os múltiplos.

21. O número que indica quantas vezes um múltiplo contém em si o número simples é chamado o *índice* do múltiplo. Assim, o índice de duplos é 2, de trios 3, de quádruplos 4, *etc*.

22. Se o número a é tomado tantas vezes, quanto o número n contém unidades, o índice do múltiplo assim produzido é n e, além disto, esse múltiplo é expresso por na, de tal modo que na denotará o múltiplo de a cujo índice é n.

23. Ainda mais, o múltiplo na, de a, é também um múltiplo do índice n, visto que contém em si o índice tantas vezes, quanto o número a contém a unidade.

24. É, portanto, claro que o múltiplo do número *a*, cujo índice é *n*, coincide com o múltiplo do número *n*, cujo índice é *a*; como o múltiplo expresso por *na* será também expresso por *an*, teremos *na* = *an*.

25. Como, em qualquer múltiplo *na*, o número *a*, do qual *na* é o múltiplo, e o índice *n* do múltiplo podem ser permutados, os dois números *a* e *n* são chamados, sem discriminação, *fatores*, enquanto o próprio múltiplo *na* costuma receber o nome de *produto* ou *resultado*.

26. Da mesma forma, qualquer número é um múltiplo da unidade, sendo o próprio número o índice do múltiplo; o número, com respeito a si mesmo, é também simples, sendo a unidade seu índice. No que segue, portanto, não consideraremos múltiplos da unidade, nem números simples, como múltiplos.

27. Para nos, portanto, múltiplos serão números do seguinte tipo: qualquer número além da unidade (e excluindo números simples) será um múltiplo e, portanto, consistirá de dois fatores, qualquer um dos quais pode ser considerado o índice com respeito ao outro.

28. O resultado *ab*, portanto, cujos fatores são *a* e *b*, é um múltiplo tanto de *a*, quanto de *b*. Como múltiplo de *a*, seu índice é *b* e, ao contrário, como múltiplo de *b*, seu índice é *a*.

29. Um múltiplo do resultado *ab* será simultaneamente um múltiplo tanto de *a*, quanto de *b*. Seja *nab* um múltiplo, cujo índice é *n*; visto que é também um múltiplo de *n*, será um múltiplo de cada um dos números *n*, *a* e *b*.

30. Disto, é também claro que, num produto contendo três fatores, os três fatores são permutáveis, de tal maneira que o resultado *abc* é não somente um múltiplo dos números individuais *a*, *b*, *c*, mas também dos fatores tomados dois a dois, *ab*, *ac*, *bc*.

31. Se, na série dos números 1, 2, 3, 4, 5, 6, 7, *etc*., todos os múltiplos forem retirados, restarão apenas números que não são múltiplos de qualquer outro número (pois excluímos os números simples da classe dos múltiplos)[1] e esses números serão chamados *símplices* ou *primos*.

32. Ao retirar os múltiplos de dois, 4, 6, 8, 10, 12, *etc*., resta a série 1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, *etc*.; em seguida, removemos os múltiplos de três 6, 9, 12, 15, 18, 21, *etc*., que ainda estão presentes, e restam 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, *etc*.; e, assim, finalmente restarão apenas números

[1] N. do Trad. Ver §26 e §27.

primos 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, *etc*.[2]

33. Se, portanto, p é um número primo, p não ocorre entre os múltiplos de dois, nem entre os múltiplos de qualquer outro número e, assim, ele não pode ser exibido como um resultado do tipo ab, a não ser que seja ou $a = 1$ ou $b = 1$, quais casos, porém, excluímos (§26).

34. Todo número que não é primo é chamado *composto*; disto, fica claro que todo número composto é múltiplo de outros números menores, que são primos, ou, de novo, múltiplos de outros menores; mas, múltiplos de qualquer produto são, ao mesmo tempo, múltiplos de seus fatores individuais e, portanto, segue que todo número composto, na análise final, é reduzido a múltiplos de números primos.

35. Todo número, portanto, é ou um número primo, ou um múltiplo de alguns números primos; como, no segundo caso, o número é composto, todo número composto pode ser exibido como um produto, cujos fatores individuais são números primos.

36. Entre os números compostos ocorrem, no primeiro lugar, os que são compostos de somente dois números primos. Se, por exemplo, p e q denotarem dois números primos

[2] N. do Trad. Observamos que aqui Euler classifica 1 como um número primo. O processo que ele descreve para achar os números primos (menores que um número N) é conhecido como o crivo de Eratóstenes.

quaisquer, o produto *pq* exibirá a forma geral dos números compostos desse primeiro tipo, os que consistem de somente dois fatores primos.

37. Assim, um número composto *pq*, desse tipo, será tanto um múltiplo do número *q*, sendo *p* o índice, quanto múltiplo do próprio *p*, sendo *q* o índice, e, de fato, não será múltiplo de qualquer outro número. Pois, se fosse múltiplo de algum outro número *a*, sendo *b* o índice, então os números *a* e *b* seriam fatores dele, o que contradiz a hipótese.

38. Um produto do tipo *pa*, porém, com fator primo *p* e fator composto *a* (tendo esse os fatores α, β, γ, *etc*.), será múltiplo não somente dos números *p* e *a*, mas também ocorrerá entre os múltiplos de α, β, γ, *etc*.

39. Depois dos números compostos consistindo de dois fatores primos, deveriam ser considerados como os próximos os que consistem de três fatores primos, cuja forma geral é, portanto, *pqr*, onde *p*, *q*, e *r* denotam números primos quaisquer.

40. Então, seguirão os números compostos que são produtos de quatro números primos, cuja forma será *pqrs*. Os seguintes tipos serão produtos consistindo ou de cinco números primos, ou de seis, ou de sete, etc.

41. Desta maneira, todos os números são distribuídos em classes, de tal forma que a primeira contém todos os números

primos; a segunda, produtos de dois primos; a terceira, produtos de três primos, a quarta, de quatro primos, a quinta, de cinco primos; e assim sucessivamente.

42. Depois da unidade, portanto, os números da primeira classe, ou seja, a dos primos, não maiores que cem, são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

43. Os números da segunda classe, menores que cem, são

$2\cdot 2 = 4$,	$3\cdot 3 = 9$,	$5\cdot 5 = 25$,	$7\cdot 7 = 49$,
$2\cdot 3 = 6$,	$3\cdot 5 = 15$,	$5\cdot 7 = 35$,	$7\cdot 11 = 77$,
$2\cdot 5 = 10$,	$3\cdot 7 = 21$,	$5\cdot 11 = 55$,	$7\cdot 13 = 91$,
$2\cdot 7 = 14$,	$3\cdot 11 = 33$,	$5\cdot 13 = 65$,	
$2\cdot 11 = 22$,	$3\cdot 13 = 39$,	$5\cdot 17 = 85$,	
$2\cdot 13 = 26$,	$3\cdot 17 = 51$,	$5\cdot 19 = 95$,	
$2\cdot 17 = 34$,	$3\cdot 19 = 57$,		
$2\cdot 19 = 38$,	$3\cdot 23 = 69$,		
$2\cdot 23 = 46$,	$3\cdot 29 = 87$,		
$2\cdot 29 = 58$,	$3\cdot 31 = 93$,		
$2\cdot 31 = 62$,			
$2\cdot 37 = 74$,			
$2\cdot 41 = 82$,			
$2\cdot 43 = 86$,			
$2\cdot 47 = 94$,			

44. Então, os números da terceira classe, menores que cem, são

$2\cdot2\cdot\ 2 = 8,$	$2\cdot3\cdot\ 3 = 18,$	$3\cdot3\cdot\ 3 = 27,$
$2\cdot2\cdot\ 3 = 12,$	$2\cdot3\cdot\ 5 = 30,$	$3\cdot3\cdot\ 5 = 45,$
$2\cdot2\cdot\ 5 = 20,$	$2\cdot3\cdot\ 7 = 42,$	$3\cdot3\cdot\ 7 = 63,$
$2\cdot2\cdot\ 7 = 28,$	$2\cdot3\cdot11 = 66,$	$3\cdot3\cdot11 = 99,$
$2\cdot2\cdot11 = 44,$	$2\cdot3\cdot13 = 78,$	
$2\cdot2\cdot13 = 52,$		$3\cdot5\cdot\ 5 = 75,$
$2\cdot2\cdot17 = 68,$	$2\cdot5\cdot\ 5 = 50,$	
$2\cdot2\cdot19 = 76,$	$2\cdot5\cdot\ 7 = 70,$	
$2\cdot2\cdot23 = 92,$	$2\cdot7\cdot\ 7 = 98,$	

45. Os números da quarta classe, abaixo de cem, são[3]

$2\cdot2\cdot2\cdot\ 2 = 16,$	$2\cdot2\cdot3\cdot3 = 36,$	$2\cdot3\cdot3\cdot3 = 54,$
$2\cdot2\cdot2\cdot\ 3 = 24,$	$2\cdot2\cdot3\cdot5 = 60,$	$2\cdot3\cdot3\cdot5 = 90,$
$2\cdot2\cdot2\cdot\ 5 = 40,$	$2\cdot2\cdot3\cdot7 = 84,$	
$2\cdot2\cdot2\cdot\ 7 = 56,$		$3\cdot3\cdot3\cdot3 = 81,$
$2\cdot2\cdot2\cdot11 = 88,$	$2\cdot2\cdot5\cdot5 = 100,$	

46. Os números da quinta classe, não maiores que cem, são

$2\cdot2\cdot2\cdot2\cdot2 = 32,$	$2\cdot2\cdot2\cdot2\cdot5 = 80,$
$2\cdot2\cdot2\cdot2\cdot3 = 48,$	$2\cdot2\cdot2\cdot3\cdot3 = 72,$

[3] N. do Trad. O texto original tem 63 para $2\cdot2\cdot3\cdot3$, o que é claramente um erro de transcrição. Observamos que $2\cdot2\cdot5\cdot5$ não é menor que cem, mas Euler evidentemente queria dizer, como no §42 e §46, "não maiores que cem".

47. Na sexta classe, ocorrem dois números desse tipo

$$2\cdot2\cdot2\cdot2\cdot2\cdot2 = 64, \qquad 2\cdot2\cdot2\cdot2\cdot2\cdot3 = 96.$$

As classes seguintes não contêm números menores que cem.

48. Os números de cada classe distinguem-se dos números das outras classes pela sua natureza específica e, assim, um determinado número pertence a uma certa classe qualquer e não pode pertencer a qualquer outra.

49. Sejam, então, *p*, *q*, *r*, *s*, *etc*. números primos; as formas dessas classes podem ser exibidas da seguinte maneira:

Forma da classe I....*p*,
« II....*pq*,
« III....*pqr*,
« IV...*pqrs*,
« V...*pqrst*,
« VI...*pqrstu*,
etc.

50. Visto que todos os números são contidos nessas classes, se estendermos a série dos números naturais 1, 2, 3, 4, *etc*. até *n*, de tal forma que a quantidade desses números seja = *n* e que a quantidade de números primos contidos nessa série seja = α, a quantidade de números da segunda classe = β, da terceira classe = γ, da quarta = δ, e assim por diante, será necessário que $\alpha+\beta+\gamma+\delta+$*etc*. = *n*. Assim, vemos que, se tomarmos *n* = 100,

teremos $\alpha = 26$ (incluindo a unidade entre os primos), $\beta = 34$, $\gamma = 22$, $\delta = 12$, $\varepsilon = 4$, $\zeta = 2$, $\eta = 0$, e temos, decerto, que $26+34+22+12+4+2 = 100$.

51. Denotando por *n* as potências de dois, a quantidade dos números até *n*, que cada classe conterá, será a seguinte:

Número	*Quantidade de números*									
n	α	β	γ	δ	ε	ζ	η	θ	ι	κ
2	2									
4	3	1								
8	5	2	1							
16	7	6	2	1						
32	12	10	7	2	1					
64	19	22	13	7	2	1				
128	32	42	30	14	7	2	1			
256	55	82	60	34	15	7	2	1		
512	98	157	125	71	36	15	7	2	1	
1024	173	304	256	152	77	37	15	7	2	1

52. Se contemplarmos atentamente a disposição dos números, perceberemos facilmente que, no início, os números primos ocorrem muito frequentemente, com os números compostos intercalados mais raramente. Na medida em que progredimos, porém, mais números compostos e, ao contrário, menos primos, serão encontrados.

53. Devemos também observar, então, que, na progressão dos números primos 1, 2, 3, 5, 7, 11, 13, 17, 19, *etc*., evidentemente não há ordem alguma pela qual uma lei de formação da progressão pode ser definida, embora, de forma geral, é certo que, o mais longe que progredimos, o menos frequentes eles se tornam.

54. Há tabelas, nas quais números primos são dispostos em relação às centenas. Assim, na primeira centena, de 1 a 100, há 26 números primos, na segunda, 21 e, nas seguintes, de fato, menos; não obstante, sua quantidade não diminui continuamente, mas é, ao contrário, completamente irregular, agora crescendo, agora decrescendo. Assim, de 200 a 300 ocorrem 16 números primos, enquanto há 17 de 400 a 500 e essa mesma quantidade de 1400 a 1500. Mais adiante, de 79700 a 79800, apenas três números primos serão encontrados; não obstante, na centena de 90000 a 90100, serão descobertos 13 números primos.

Capítulo II

Sobre divisores de números

55. Quando um certo número é um múltiplo de outro número, o referido outro número é chamado *divisor* do primeiro, e o índice da multiplicação é geralmente chamado o *quociente* surgido da divisão.

56. Assim, se o número N for um múltiplo de a, sendo o índice n, de tal modo que tenhamos $N = na$, o número a será um divisor do número N e o índice n fornecerá o quociente. Isto é, se o número $N = na$ for dividido por a, o quociente será n.

57. Visto que os números n e a são permutáveis e, neste respeito, são chamados fatores, o número $N = na$ também terá n como divisor e, neste caso, seu quociente será a. Em geral, portanto, o divisor multiplicado pelo quociente reproduz o próprio número que foi dividido.

58. Visto que qualquer número é seu próprio número simples, a unidade é divisor de todo número, sendo o próprio número o quociente. Em consequência, qualquer número é seu próprio divisor, sendo o quociente a unidade.

59. Portanto, um número qualquer N terá, primeiro, a unidade como seu divisor e terá o próprio número N como

quociente. Então, um número qualquer *N* também terá se mesmo como divisor, sendo o quociente a unidade.

60. Nenhum número tem outros divisores, exceto os dos quais é um múltiplo (aqui não excluo o número simples da ideia de múltiplo); pois, se tivesse outro divisor, já seria, em virtude disto, um múltiplo desse divisor, sendo o índice do múltiplo fornecido pelo quociente.

61. Visto, portanto, que um número primo não é múltiplo de qualquer outro número, além da unidade, um número primo não tem outros divisores além da unidade e se mesmo. Isto é, se *p* for um número primo, seus divisores serão 1 e *p* e ele não terá qualquer outro além desses.

62. Números primos, portanto, ou números da primeira classe, têm apenas dois divisores, exceto a unidade, que, decerto, tem apenas um; por esta razão, a unidade geralmente não é incluída entre os números primos.

63. Números da segunda classe, que consistem de dois fatores primos *pq*, porque são múltiplos de cada um dos mesmos, têm, além dos divisores 1 e *pq*, também os divisores *p* e *q*, de tal forma que todos seus divisores são 1, *p*, *q*, e *pq*.

64. Porém, o caso em que os fatores *p* e *q* são iguais deve ser considerado à parte, pois não é permitido contar o mesmo número entre os divisores duas vezes. Assim, o número *pp*, que

é o quadrado de um número primo, tem apenas três divisores 1, p e pp.

65. Por essa razão, convém subdividir os números da segunda classe em dois tipos, dos quais o primeiro contém números da forma pp e tem três divisores, 1, p e pp; o outro tipo contém números da forma pq, onde as letras p e q denotam números primos distintos. Os números desse tipo terão os quatro divisores 1, p, q, pq.

66. De forma análoga, a terceira classe deve ser subdividida em três tipos, cujas formas são p^3, p^2q e pqr, onde p, q, r denotam números primos distintos, pois ou todos os três fatores são iguais, ou somente dois, ou todos os três são desiguais.

67. Assim, para a terceira classe de números,

o primeiro tipo p^3 terá os quatro divisores $1, p, p^2, p^3$,
segundo p^2q seis $1, p, q, p^2, pq, p^2q$,
terceiro pqr oito $1, p, q, r, pq, pr, qr, pqr$,

e não pode haver quaisquer outros divisores nesse classe.

68. A quarta classe, que contém números consistindo de quatro fatores primos, visto que pode ter ou dois, ou três ou todos os quatro desses fatores iguais, deve ser subdividida em cinco tipos, cujas formas são I. p^4, II. p^3q, III. p^2q^2, IV. p^2qr, V. $pqrs$.

69. Agora será fácil enumerar todos os divisores de cada tipo da quarta classe:

Tipos		os divisores serão
I. p^4	cinco:	$1, p, p^2, p^3, p^4,$
II. p^3q	oito:	$1, p, q, p^2, pq, p^3, p^2q, p^3q,$
III. p^2q^2	nove:	$1, p, q, p^2, pq, q^2, p^2q, pq^2, p^2q^2$
IV. p^2qr	doze:	$1, p, q, r, p^2, pq, pr, qr, p^2q, p^2r, pqr, p^2qr,$
V. $pqrs$	dezesseis:	$1, p, q, r, s, pq, pr, ps, qr, qs, rs, pqr, pqs, prs, qrs, pqrs.$

70. Para a quinta classe, que reuni números compostos de cinco fatores primos, devido à igualdade de alguns dos fatores, devemos listar os seguintes tipos:

I. p^5, II. p^4q, III. p^3q^2, IV. p^3qr, V. p^2q^2r, VI. p^2qrs, VII. $pqrst$.

71. Então, os divisores desses tipos serão enumerados da seguinte maneira:

Tipos		os divisores serão
I. p^5	seis:	$1, p, p^2, p^3, p^4, p^5,$
II. p^4q	dez:	$1, p, q, p^2, pq, p^3, p^2q, p^4, p^3q, p^4q,$
III. p^3q^2	doze:	$1, p, q, p^2, pq, q^2, p^3, p^2q, pq^2, p^3q, p^2q^2, p^3q^2,$
IV. p^3qr	dezesseis:	$1, p, q, r, p^2, pq, pr, qr, p^3, p^2q, p^2r, pqr, p^3q, p^3r, p^2qr, p^3qr,$
V. p^2q^2r	dezoito:	$1, p, q, r, p^2, pq, pr, q^2, qr, p^2q, p^2r, pq^2, pqr, q^2r, p^2q^2, p^2qr, pq^2r, p^2q^2r,$

VI. p^2qrs vinte e quatro: $1, p, q, r, s, p^2, pq, pr, ps, qr, qs, rs, p^2q, p^2r, p^2s, pqr, pqs, prs, qrs, p^2qr, p^2qs, p^2rs, pqrs, p^2qrs,$

VII. $pqrst$ trinta e dois: $1, p, q, r, s, t, pq, pr, ps, pt, qr, qs, qt, rs, rt, st, pqr, pqs, pqt, prs, prt, pst, qrs, qrt, qst, rst, pqrs, pqrt, pqst, prst, qrst, pqrst.$

72. Os tipos das classes restantes serão constituídos de forma semelhante e todos seus divisores serão classificados em diversos tipos. E, ao mesmo tempo, a natureza dos vários divisores será revelada por esse procedimento, bem como tanta a classe, quanto o tipo, aos quais cada um deve ser referido.

73. Sejam $1, \alpha, \beta, \gamma, \delta, ..., N$, os divisores do número N e seja o mesmo multiplicado por um número primo p, que não é nele contido. Então, o produto Np terá como divisores, além dos já mencionados $1, \alpha, \beta, \gamma, \delta, ..., N$, esses mesmos por p multiplicados, $p, \alpha p, \beta p, \gamma p, \delta p, ..., Np$, e, assim, a quantidade dos seus divisores será o dobro.

74. Mas, se o número N for multiplicado pelo quadrado de um número primo p, que não consta no mesmo como fator, a quantidade de divisores será triplicada. Pois, o produto Np^2 terá, primeiro, os mesmos divisores de N, segundo, os mesmos multiplicados por p e, terceiro, os mesmos multiplicados por p^2.

75. De forma semelhante, se p for um número primo não contido em N, e se o número N for multiplicado por p^3, o produto Np^3 terá, primeiro, todos os divisores do número N, então os mesmos multiplicados por p, em seguida os mesmos multiplicados por p^2 e, finalmente, os mesmos multiplicados por p^3, de tal forma que a quantidade de divisores do produto Np^3 é quatro vezes maior que a do número N.

76. De forma geral, se a quantidade de divisores do número N for $= m$ e se for multiplicado pela potência p^λ de um número primo p, a quantidade de divisores do produto Np^λ será $(\lambda+1)m$; será útil observar que, por isto, a quantidade de divisores da própria potência p^λ é $\lambda+1$.

77. De tudo isto, é claro que há uma regra conveniente, que determina a quantidade de divisores de qualquer número. Seja $p^\lambda q^\mu r^\nu s^\xi$ a forma do número proposto. Visto que a quantidade de divisores do número p^λ é $\lambda+1$, a quantidade de divisores do número $p^\lambda q^\mu$ será $(\lambda+1)(\mu+1)$, a do número $p^\lambda q^\mu r^\nu$ será $(\lambda+1)(\mu+1)(\nu+1)$ e, finalmente, a do número $p^\lambda q^\mu r^\nu s^\xi$ será $(\lambda+1)(\mu+1)(\nu+1)(\xi+1)$. Mais ainda, a classe, à qual o referido

número pertence, é indicada pelo número $\lambda+\mu+\nu+\xi$, ou seja, a soma[1] dos expoentes.

78. Portanto, infinitos números, que têm uma quantidade dada de divisores, podem ser exibidos. Pois, seja a quantidade de divisores = a, onde a é um número primo[2]; os números procurados são contidos na forma p^{a-1}, onde p denota um número primo qualquer.

79. Se a, b, c, d, *etc*., bem como as letras p, q, r, s, *etc*., denotam números primos, os números tendo a quantidade ab de divisores são ou p^{ab-1}, ou $p^{a-1}q^{b-1}$; os tendo a quantidade abc de divisores são ou p^{abc-1}, ou $p^{ab-1}q^{c-1}$, ou $p^{ac-1}q^{b-1}$, ou $p^{bc-1}q^{a-1}$, ou $p^{a-1}q^{b-1}r^{c-1}$, onde as letras a, b, c, *etc*, podem significar quaisquer números primos, sob a condição que p, q, r, *etc*. sejam distintos.

80. Assim, se a quantidade de divisores seja = 2, somente números primos serão satisfatórios, ou seja, números contidos na forma p. Mas, se tivermos

[1] N. do Trad. Ver §49. Observe que os primos que definem a classe no referido parágrafo não são necessariamente distintos.

[2] N. do Trad. Se a for composto, p^{a-1}, para p primo, ainda terá a divisores. No entanto, haverá outras formas que também têm a divisores. Ver o próximo parágrafo. Quando a é primo, no entanto, isto não pode acontecer, pois se tivéssemos, por exemplo, $p^{b-1}q^{c-1}$, para expoentes não triviais, teríamos $a = bc$, e a não seria primo.

quantidade de divisores:	a forma dos números será:
3	p^2
4	p^3, pq
5	p^4
6	p^5, p^2q
7	p^6
8	p^7, p^3q, pqr
9	p^8, p^2q^2
10	p^9, p^4q
11	p^{10}
12	$p^{11}, p^5q, p^3q^2, p^2qr$.

81. Se, portanto, a forma (ou seja, a classe e o tipo a que pertence) de qualquer número seja conhecida, não somente a quantidade dos seus divisores, mas também os próprios divisores, podem ser exibidas através do recurso das regras[3].

[3] N. do Trad. A regra para a quantidade dos divisores é dada no §77 e a para os divisores em §69 a §71.

Capítulo III

Sobre a soma dos divisores de qualquer número

82. Dado qualquer número n, designaremos a soma de todos seus divisores por $\int n$, de tal forma que o símbolo $\int n$ denota a soma dos divisores de n.

83. Visto que a unidade não tem outros divisores além de si mesmo, teremos que $\int 1 = 1$. A soma dos divisores de qualquer outro número será maior que si mesmo, isto é, teremos, com certeza, $\int n > n$, exceto para $n = 1$.

84. Para números primos p, visto que não admitem outros divisores além de si mesmo e a unidade, teremos $\int p = p+1$. Mais ainda, teremos, para potências de números primos,

$$\int p^1 = p+1 = \frac{pp-1}{p-1},$$

$$\int p^2 = pp+p+1 = \frac{p^3-1}{p-1},$$

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

e em geral

$$\int p^n = p^n+p^{n-1}+p^{n-2}+\ldots+1 = \frac{p^{n+1}-1}{p-1}.$$

85. Visto que os divisores de números contidos na forma pq são $1, p, q, pq$, sua soma será

$$1+p+q+pq = (1+p)(1+q) \text{ e, portanto, } \int pq = (p+1)(q+1).$$

De forma semelhante, teremos, para os da terceira classe,

$$\int p^2q = (pp+p+1)(q+1) \text{ e } \int pqr = (p+1)(q+1)(r+1).$$

86. Os divisores das outras classes podem ser somados do mesmo modo. Para que a natureza dessas somas seja examinada mais claramente, consideremos o número geral N, cujos divisores são $1, \alpha, \beta, \gamma, \delta, \ldots, N$ e cuja soma é $\int N$. Ao multiplicar o mesmo por um número primo p, nele não contido, o produto Np terá, além dos referidos divisores, os mesmos multiplicados por p, cuja soma, portanto, será $p\int N$; somando aos outros[1], temos $\int Np = (p+1)\int N = \int p \int N$.

87. Da mesma maneira em que foi feito em §74, se um número N for multiplicado pelo quadrado de um número primo p, nele não contido, a soma dos divisores do produto Np^2 será

$(1+p+p^2)\int N$, ou seja, $\int Np^2 = \int N \int p^2$;

e, do mesmo modo, teremos $\int Np^3 = \int N \int p^3$ e assim por diante.

88. Assim, as somas dos divisores para as diversas classes e tipos serão expressas da seguinte maneira:

[1] N. do Trad. Isto é, $\int Np = p\int N + \int N$.

$$\int p = 1+p$$
$$\int p^2 = 1+p+p^2$$
$$\int pq = (1+p)(1+q)$$
$$\int p^3 = 1+p+p^2+p^3$$
$$\int p^2q = (1+p+p^2)(1+q)$$
$$\int pqr = (1+p)(1+q)(1+r)$$
$$\int p^4 = 1+p+p^2+p^3+p^4$$
$$\int p^3q = (1+p+p^2+p^3)(1+q)$$
$$\int p^2q^2 = (1+p+p^2)(1+q+q^2)$$
$$\int p^2qr = (1+p+p^2)(1+q)(1+r)$$
$$\int pqrs = (1+p)(1+q)(1+r)(1+s)$$
etc.

89. Dessas fórmulas, deduzimos[2] as seguintes conclusões:

$$\int p^2 = p^2+\int p = 1+p\int p$$
$$\int p^3 = p^3+\int p^2 = 1+p\int p^2 = 1+p+p^2\int p$$
$$\int p^4 = 1+p\int p^3 = 1+p+p^2\int p^2 = 1+p+p^2+p^3\int p$$
$$\int p^5 = 1+p\int p^4 = 1+p+p^2\int p^3 = 1+p+p^2+p^3\int p^2 = 1+p+p^2+p^3+p^4\int p$$
etc.

das quais é evidente que, em geral, temos

$$\int p^n = 1+p\int p^{n-1} = 1+p+p^2\int p^{n-2} = 1+p+p^2+p^3\int p^{n-3}\ etc.$$

[2] N. do Trad. De $\int p^2 = p^2+\int p$ obtemos $p^3+p\int p = p\int p^2 = p(1+p+p^2) = p+p^2+p^3$ e, portanto, $p\int p = p+p^2$. Somando a unidade aos dois lados dessa equação e substituindo para o lado direito, obtemos $1+p\int p = \int p^2$. Para $n > 2$, a primeira relação é obtida de maneira semelhante e os demais por substituição de valores já obtidos para $p^k\int p^n$.

90. Seja dado, então, um número N, para o qual devemos determinar a soma dos seus divisores. Seja N decomposto nos seus fatores primos, de modo que

$$N = p^{\lambda}q^{\mu}r^{\nu}s^{\xi}, \quad \text{do qual teremos} \quad \int N = \int p^{\lambda} \cdot \int q^{\mu} \cdot \int r^{\nu} \cdot \int s^{\xi}.$$

91. Portanto, uma vez que podemos determinar as somas dos divisores tanto dos próprios números primos, quanto das suas potências, é claro que as somas dos divisores de todos os números podem ser determinadas.

92. Para um número primo p, visto que $\int p = p+1$, a soma dos seus divisores sempre será um número par, exceto para $p = 2$, em qual caso temos $\int 2 = 3$. Pois, para $p = 2a-1$, teremos $\int(2a-1) = 2a$. Ainda mais, porque $\int p^2 = p^2+p+1$, a soma dos divisores do quadrado de qualquer número primo sempre será um número ímpar e, muitas vezes, até um número primo, como por exemplo $\int 2^2 = 7$, $\int 3^2 = 13$, $\int 5^2 = 31$.

93. Continuando, se N for o cubo de um número primo, ou seja,

$$N = p^3, \quad \text{teremos} \quad \int p^3 = = 1+p+pp+p^3 = (1+p)(1+pp),$$

logo, será um número composto e, exceto para $p = 2$, a soma dos divisores será, no mínimo, divisível por 4, pois cada fator $1+p$ e $1+pp$ é par. Teremos, então, $\int p^3 = (1+pp)\int p$.

94. Se o número N for a quarta potência de um número primo, ou seja, $N = p^4$, a soma dos divisores será $\int p^4 =$

$1+p+pp+p^3+p^4$ e, portanto, sempre ímpar, e até pode acontecer que seja um número primo, como por exemplo $\int 2^4 = 31$.

95. Seja $N = p^5$. Como $\int p^5 = 1+p+pp+p^3+p^4+p^5$, a soma dos divisores será

$$\int p^5 = (1+p+pp)(1+p^3) = (1+p)(1+p+pp)(1-p+pp)$$

e, portanto, é um número composto, sendo composto de somas de potências menores, visto que

$$\int p^5 = (1-p+pp)\int p \int p^2.$$

96. Seja proposto agora o produto MN, cujos fatores M e N não têm fator primo algum em comum. Teremos $\int MN = \int M \cdot \int N$; logo, a soma dos divisores será ainda mais composta, quanto mais números primos distintos são incluídos.

97. Seja proposto qualquer número N, a soma de cujos divisores é $\int N$. Se o mesmo é multiplicado por um número primo p, a soma dos divisores do produto Np sempre é maior que $p\int N$. Pois, $\int Np$ é compreendida primeiro por todos os divisores do número N multiplicados por p, cuja soma é $p\int N$, e depois também pelos divisores do número N sem serem multiplicados por p.

98. A demonstração tem duas partes. Primeiro, se o número primo p não for contido em N, certamente teremos $\int Np$

$= \int p \cdot \int N = (1+p)\int N = p\int N + \int N$, em qual caso temos, sem dúvida, $\int Np > p\int N$.

99. E se p for de fato contido em N, de tal maneira que $N = Mp^n$, teremos $\int N = \int M \cdot \int p^n$; mas $\int Np = \int M \int p^{n+1}$. Mas, do que foi estabelecido acima[3], temos que $\int p^{n+1} = 1 + p\int p^n$, do qual deduzimos $\int Np = \int M + p\int p^n \int M$ e, assim, temos $\int Np = p\int N + \int M$ e, portanto, $\int Np > p\int N$.

100. As somas dos divisores dos números naturais, na ordem da sua progressão, são as seguintes:

$\int 1 = 1$	$\int 13 = 14$	$\int 25 = 31$	$\int 37 = 38$	$49 = 57$
$\int 2 = 3$	$\int 14 = 24$	$\int 26 = 42$	$\int 38 = 60$	$\int 50 = 93$
$\int 3 = 4$	$\int 15 = 24$	$\int 27 = 40$	$\int 39 = 56$	$\int 51 = 72$
$\int 4 = 7$	$\int 16 = 31$	$\int 28 = 56$	$\int 40 = 90$	$\int 52 = 98$
$\int 5 = 6$	$\int 17 = 18$	$\int 29 = 30$	$\int 41 = 42$	$\int 53 = 54$
$\int 6 = 12$	$\int 18 = 39$	$\int 30 = 72$	$\int 42 = 96$	$\int 54 = 120$
$\int 7 = 8$	$\int 19 = 20$	$\int 31 = 32$	$\int 43 = 44$	$\int 55 = 72$
$\int 8 = 15$	$\int 20 = 42$	$\int 32 = 63$	$\int 44 = 84$	$\int 56 = 120$
$\int 9 = 13$	$\int 21 = 32$	$\int 33 = 48$	$\int 45 = 78$	$\int 57 = 80$
$\int 10 = 18$	$\int 22 = 36$	$\int 34 = 54$	$\int 46 = 72$	$\int 58 = 90$
$\int 11 = 12$	$\int 23 = 24$	$\int 35 = 48$	$\int 47 = 48$	$\int 59 = 60$
$\int 12 = 28$	$\int 24 = 60$	$\int 36 = 91$	$\int 48 = 124$	$\int 60 = 168$

[3] N. do Trad. Em §89.

101. Nem todo número ocorre entre essas somas de divisores e, de fato, até 60, os seguintes são excluídos:

2, 5, 9, 10, 11, 16, 17, 19, 21, 22, 23, 25, 26, 27, 29, 33, 34, 35, 37, 41, 43, 45, 46, 47, 49, 50, 51, 52, 53, 55, 58, 59.

Desta forma, os números que exprimem somas de divisores são:

1, 3, 4, 6, 7, 8, 12, 13, 14, 15, 18, 20, 24, 28, 30, 31, 32, 36, 38, 39, 40, 42, 44, 48, 54, 56, 57, 60.

102. Disto, é claro que dois ou mais números podem fornecer a mesma soma de divisores, por exemplo,

$\int 6 = \int 11 = 12$
$\int 10 = \int 17 = 18$
$\int 16 = \int 25 = 31$
$\int 21 = \int 31 = 32$
$\int 34 = \int 53 = 54$
$\int 28 = \int 39 = 56$

$\int 14 = \int 15 = \int 23 = 24$
$\int 20 = \int 26 = \int 41 = 42$
$\int 33 = \int 35 = \int 47 = 48$
$\int 24 = \int 38 = \int 59 = 60.$

103. Costuma-se propor o problema em que o número procurado faz uma certa razão com a soma das suas divisores; isto é, devemos ter $N{:}\int N = n{:}m$, ou seja, $\frac{\int N}{N} = \frac{m}{n}$, onde estipulamos que $m > n$; pois, se tivéssemos $m = n$, teríamos $N = 1$.

104. Sendo a razão $m{:}n$ irredutível, o número N será igual ou ao próprio n, ou a algum múltiplo do mesmo. Seja, então, $N = an$; teremos $\int N = \int an = am$. Mas, exceto para $a = 1$,

temos[4] $\int an > a\int n$ e, assim, $m > \int n$. Desta forma, se tivermos $m < \int n$, não haverá solução alguma; para $m = \int n$, contudo, há uma solução única, a saber, $N = n$.

105. Logo, exceto para ou $m = \int n$, ou $m > \int n$, o problema não admite solução. No primeiro caso, decerto, o número procurado, N, será igual ao próprio n e não terá qualquer outra solução. No segundo caso, em que $m > \int n$, se de fato houver uma solução, o número N será igual a um certo múltiplo do próprio n, digamos $N = an$. De qualquer forma, dado uma razão $m{:}n$, o problema ainda pode não ter solução, mesmo se $m > \int n$.

106. Um número é *perfeito* se a soma dos seus divisores é o dobro do próprio número. Assim, se tivermos $\int N = 2N$, então N será um número perfeito. Se o mesmo for par, ele será $2^n A$, sendo A um número ímpar, ou primo ou composto. Sendo, então

$$N = 2^n A, \text{ teremos } \int N = (2^{n+1}-1)\int A = 2^{n+1} A,$$

$$\text{do qual temos } \frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1}-1}.$$

107. Porque o numerador da fração $\frac{2^{n+1}}{2^{n+1}-1}$ supera o denominador apenas por uma unidade, ele não pode exceder a

[4] N. do Trad. Ver §97.

soma dos divisores do denominador[5]; será, portanto, ou igual ou menor. No segundo caso não há solução e, na verdade, não há solução no primeiro caso, exceto quando $2^{n+1}-1$ for um número primo. Sempre que $2^{n+1}-1$ for um número primo, A deverá ser tomado como sendo igual ao mesmo e teremos o número perfeito = $2^n(2^{n+1}-1)$.

108. Todo número perfeito par, portanto, é contido na fórmula $2^n(2^{n+1}-1)$, sob a condição de que $2^{n+1}-1$ seja um número primo, o que não pode ocorrer, contudo, se $n+1$ não seja um número primo[6]; no entanto, nem todo número primo, quando substituído no lugar de $n+1$, faz com que $2^{n+1}-1$ seja primo. Até agora, ninguém tem demonstrado se haja, ou não, além desses números perfeitos pares, também ímpares.

109. Se houver um número perfeito ímpar, todos os seus fatores serão necessariamente ímpares. Seja, então, ele = $ABCD$ *etc*. e devemos ter $\int A \cdot \int B \cdot \int C \cdot \int D = 2ABCD$, um número imparmente[7] par. Logo, só pode ter um único número imparmente par entre as somas dos divisores $\int A$, $\int B$, $\int C$, $\int D$, todos os outros sendo ímpares. Portanto, todos os fatores A, B, C, D, exceto um, serão potências pares de números primos e,

[5] N. do Trad. Isto é, 2^{n+1} não excede $\int(2^{n+1}-1)$ e essa soma é, *no mínimo*, $(2^{n+1}-1)+1$, ou seja, 2^{n+1}. O resto do argumento se apóia em §104, pois $2^{n+1}/2^{n+1}-1$ é irredutível.
[6] N. do Trad. Observe que 2^a-1 divide $2^{ab}-1$.
[7] N. do Trad. Um número da forma $2(2q+1)$, para $q \geq 1$. É também chamado "par-vezes-ímpar" ou "par-ímpar".

ainda mais, aquele um será ou um número primo da forma $4n+1$, ou alguma potência do mesmo cujo expoente é $4\lambda+1$. E, assim, um número perfeito desse tipo terá a forma $(4n+1)^{4\lambda+1}PP$, onde P é um número ímpar e $4n+1$ é primo[8].

110. Omito muitos outros problemas que poderiam ser incluídos aqui, nos quais é proposto investigar outras relações entre números e as somas dos seus divisores, pois não será difícil obter um método para resolvê-los a partir dos princípios aqui expostos.

[8] N. do Trad. Se A é um primo da forma $4n+3$, então $\int A$ será divisível por 4; o mesmo acontece quando o expoente assume a forma $4\lambda+3$.

Capítulo IV

Sobre números primos e compostos entre si

111. Dois números, que não têm, além da unidade, qualquer outro fator ou divisor comum, são chamados *primos entre si*; mas os que têm, além da unidade, outro divisor comum são chamados *compostos entre si*. Assim, 8 e 15 são números primos entre si, enquanto 9 e 15 são números compostos entre si.

112. A unidade, portanto, é primo com todos os números. Denotando por n um número qualquer, os números 1 e n são claramente primos entre si, pois não admitem qualquer outro divisor comum além da unidade.

113. Da mesma maneira, dois números, n e $n+1$, que diferem por uma unidade, são primos entre si; pois, quaisquer que sejam os divisores que n tenha, nenhum deles pode dividir $n+1$. Pois, se p for um divisor do número n, o próximo número maior que é divisível por p será $n+p$ e, assim, $n+1$ não admite[1] divisão por p.

114. Um número primo p é primo com todos os números, exceto os que são múltiplos dele; desta forma, os números a e p são primos entre si, exceto no caso em que ou $a = p$ ou $a = np$.

[1] N. do Trad. Veja §14.

Portanto, o número primo p é primo com todos os números menores que si.

115. A quantidade de números menores de um dado número a é $a-1$ e vale a pena determinar quantos deles são primos com a e quantos são com ele compostos[2]; pois, disto, é fácil estender o resultado para todos os números maiores que a.

116. Pois, seja $b < a$. Se b e a forem primos entre si, então também todos os números $b+a$, $b+2a$, $b+3a$, *etc*., serão primos com a. Mas, se b e a tiveram um divisor comum, o mesmo será divisor dos números $b+a$, $b+2a$, *etc*.

117. Portanto, se $a = p$ é um número primo, visto que todos os números menores que o mesmo são primos com ele, essa quantidade é $= p-1$.

118. Seja[3] $a = 2p$. Entre 1 e a, há p números pares, os quais, portanto, não são primos com a; também o próprio número p não é primo com a. Removendo esses, cuja quantidade é $= p$, de todos os números de 1 até[4] a, restam $p-1$, e esse tanto será primo com a.

---

[2] N. do Trad. A frase "a é composto com b", muito usada no que segue, quer dizer que "a e b são números compostos entre si". É paralela à frase "a é primo com b." Em especial, a frase "a é composto com b" não implica que b (necessariamente) faz parte da composição de a.

[3] N. do Trad. Os dois fatores considerados no presente parágrafo, bem como nos próximos três, devem ser concebidos como primos entre si, como o próprio Euler esclarece em §122.

[4] N. do Trad. A frase "de 1 até a" deve ser entendido como 1, 2, ..., a.

119. Seja $a = 3p$. Entre os números não maiores que o mesmo, os que são divisíveis por 3, cuja quantidade é $= p$, não são primos com a;. ainda mais, p e $2p$ não são primos com a. Todos os restantes, cuja quantidade é $3p–p–2 = 2(p–1)$, serão primos com $a = 3p$.

120. De forma semelhante, se $a = 5p$, os números que têm um divisor comum com a são, em primeiro lugar, todos os que são divisíveis por 5, cuja quantidade é $= p$, e, ainda mais, os que são divisíveis por p, a saber, p, $2p$, $3p$ e $4p$; pois o próprio número $5p$ já foi contado. Assim, a quantidade de números compostos com a é $p+4$ e, portanto, a quantidade de números primos com a é $= 4p–4 = 4(p–1)$, isto é, claramente, os que não são maiores que o próprio a.

121. De forma mais geral, seja $a = pq$, sendo cada um dos fatores p e q primos. Da unidade até a, há p números divisíveis por q, a saber, q, $2q$, $3q$, ..., pq. Ainda há q números divisíveis por p, a saber, p, $2p$, $3p$, ..., qp, dos quais o último, qp, já foi contado. Logo, a quantidade de todos os números que não superam a e que são compostos com a será $= p+q–1$. Os restantes, portanto, cuja quantidade é

$$= qp–p–q+1 = (p–1)(q–1),$$

serão primos com a.

122. Aqui tomamos, contudo, números primos distintos por p e q. Mas, se tivéssemos $a = pp$, nenhum número seria composto com a, exceto os que são divisíveis por p, cuja quantidade é $= p$; a quantidade dos restantes, que são primos com p, será $= pp - p = p(p-1)$.

123. De modo semelhante, seja $a = p^3$. Visto que a não tem outro divisor primo além de p, todos os números de 1 até a e compostos com a são p, $2p$, $3p$, ..., p^2p, cuja quantidade é p^2; todos os números restantes, cuja quantidade é $p^3 - p^2 = p^2(p-1)$, serão primos com a.

124. Disto é claro que, em geral, se a for uma potência qualquer p^n de um número primo p, a quantidade de números primos com a, que decerto não são maiores que a, será $p^{n-1}(p-1)$.

125. Seja $a = p^2q$, sendo p e q números primos distintos. Então, visto que a não tem outros divisores primos além de p e q, os números compostos com a serão ou divisíveis por p, sendo eles p, $2p$, $3p$, ..., $pq \cdot p$, em quantidade $= pq$, ou divisíveis por q, sendo esses q, $2q$, $3q$, ..., $p^2 \cdot q$, em quantidade $= p^2$. Entre os últimos, contudo, ocorrem pq, $2pq$, $3pq$, ..., $p \cdot pq$, que já foram contados, em quantidade $= p$, de tal forma que a quantidade de todos os compostos com a é $= pq + p^2 - p$. Assim, todos os restantes, cuja quantidade é $ppq - pq - pp + p = p(p-1)(q-1)$, serão todos os primos com a.

126. Se $a = pqr$, sendo p, q, r números primos distintos, então os números compostos com a são divisíveis

1) por p, a saber, p, $2p$, $3p$, ..., $qr \cdot p$, em quantidade qr

2) por q, « q, $2q$, $3q$, ..., $pr \cdot q$, « pr

3) por r, « r, $2r$, $3r$, ..., $pq \cdot r$, « pq.

Aqui, porém, os seguintes foram contados duas vezes: os divisíveis por pq, em quantidade r, os divisíveis por pr, em quantidade q, e finalmente os divisíveis por qr, em quantidade p; estes devem ser removidos[5]. Ao fazê-lo, no entanto, o próprio número pqr foi completamente removido e, portanto, tem que ser colocado de novo. Assim sendo, a quantidade de números compostos com a será $qr+pr+pq-r-q-p+1$; logo, os restantes, cuja quantidade é

$$pqr-qr-pr-pq+r+q+\text{p}-1 = (p-1)(q-1)(r-1),$$

serão primos com o número $a = pqr$.

127. Destes dados, concluímos que, para todos os tipos dos números, teremos:

[5] N. do Trad. Isto é, devem ser removidos da lista dos números compostos com *pqr*. Logo em seguida, Euler explica que o próprio *pqr* aparece, no primeiro estágio do processo, três vezes na lista dos compostos. Mas, no segundo estágio, é retirado da lista três vezes e, consequentemente, deve ser colocado na lista de novo.

se o número proposto for	a quantidade de números menores que a e primos com ele será
$a = p$	$p-1$
$a = p^2$	$p(p-1)$
$a = pq$	$(p-1)(q-1)$
$a = p^3$	$p^2(p-1)$
$a = p^2q$	$p(p-1)(q-1)$
$a = pqr$	$(p-1)(q-1)(r-1)$
$a = p^4$	$p^3(p-1)$
$a = p^3q$	$p^2(p-1)(q-1)$
$a = p^2q^2$	$p(p-1)q(q-1)$
$a = p^2qr$	$p(p-1)(q-1)(r-1)$
$a = pqrs$	$(p-1)(q-1)(r-1)(s-1)$

128. Para que essa conclusão possa ser mais firmemente corroborada, porém, e para não confiarmos demais em indução[6], consideremos a forma $a = Mp$, onde M é um número qualquer e p um primo não contido em M. Seja μ a quantidade de números entre 1 e M que são primos com M e, portanto, a quantidade de números compostos com M é $= M-\mu$.

129. Visto que há $M-\mu$ números compostos com M entre 1 e M, terá[7] $p(M-\mu)$ números compostos com M entre 1 e Mp e esses serão, portanto, também compostos com Mp. Mas, além desses, os seguintes números são compostos com Mp: p, $2p$, $3p$, ..., Mp, em quantidade M, dos quais devem ser removidos os que já foram compostos com M, cuja quantidade é $M-\mu$; restam,

[6] N. do Trad. Isto é, "indução" por casos, não indução matemática.
[7] N. do Trad. Ver §116.

portanto, apenas μ números que são compostos com Mp, mas não com M. Deste modo, a quantidade total de números entre 1 e Mp e compostos com Mp será a seguinte: $p(M-\mu)+\mu$, e os restantes, cuja quantidade é $Mp-p(M-\mu)-\mu = \mu(p-1)$, serão primos com Mp.

130. De modo semelhante, mostra-se que, se o número proposto seja $= Mp^n$, sendo p um número primo não contido em M e sendo μ a quantidade de números primos com M, contidos entre os limites de 1 e M, então a quantidade de números menores que Mp^n e primos com Mp^n será $= p^{n-1}\mu(p-1)$.

131. Pois, procuremos os números compostos com Mp^n, os quais serão os que são compostos ou com M ou com p. E, de fato, a quantidade de números compostos com M entre 1 e Mp^n é $= p^n(M-\mu)$, enquanto os que são compostos com p serão os seguintes: p, $2p$, $3p$, ..., $Mp^{n-1}\cdot p$, em quantidade Mp^{n-1}. Destes, porém, devemos excluir os que já foram compostos com M, cuja quantidade é $p^{n-1}(M-\mu)$; desta forma, a quantidade dos que são compostos com Mp^n, mas não com M, será $= Mp^{n-1}-p^{n-1}(M-\mu) = p^{n-1}\mu$. Assim, a quantidade total de números de 1 até Mp^n, compostos com Mp^n, é $= p^n(M-\mu)+p^{n-1}\mu$. Em consequência, os restantes, cuja quantidade é $Mp^n-p^n(M-\mu)-p^{n-1}\mu = p^{n-1}\mu(p-1)$, serão primos com Mp^n.

132. Portanto, visto que a quantidade de números primos com p^n e menores que o mesmo são $= p^{n-1}(p-1)$, podemos concluir com o máximo rigor, da proposição precedente, o seguinte: se o número proposto for $= p^{\lambda}q^{\mu}r^{\nu}s^{\xi}$ *etc*., então a quantidade de todos os números que são primos com este e menores que o mesmo será

$$= p^{\lambda-1}(p-1)\cdot q^{\mu-1}(q-1)\cdot r^{\nu-1}(r-1)\cdot s^{\xi-1}(s-1)\ etc.$$

133. Se, portanto, M e N forem números primos entre si, e a quantidade de números de 1 até M, primos com M, for $= m$, enquanto a quantidade de números de 1 até N, primos com N, for $= n$, então a quantidade de números primos com o produto MN e não maiores com o mesmo será $= mn$.

134. Disto, é claro que a quantidade de todos os números primos, como Euclides já havia demonstrado[8], não pode ser finita. Pois, se o último e maior número primo fosse $= p$, poríamos o número M igual ao produto de todos os números primos, $M = 2\cdot3\cdot5\cdot7\cdot...\cdot p$, que claramente é composto com todos os números; visto, porém, que o mesmo número M é certamente primo com $M-1$ ou com $M+1$, é claro que a proposição é absurda.[9]

[8] N. do Trad. Proposição 20 do Livro IX de *Os Elementos*.
[9] N. do Trad. Nos seguintes cinco parágrafos, Euler continua a procurar contradições a partir da hipótese falsa de que a quantidade de primos é finita.

135. Do que foi feito[10], é também claro que, entre os números menores que o referido M, não somente o número M–1, mas também muitos outros, são, com certeza, primos com M, pois a quantidade desses números primos com M é = $1\cdot2\cdot4\cdot6\cdot\ldots\cdot(p-1)$, que é maior que a quantidade de números primos que são fatores de M.

136. Ponhamos $m = 1\cdot2\cdot4\cdot6\cdot\ldots\cdot(p-1)$, sendo $M = 2\cdot3\cdot5\cdot7\cdot\ldots\cdot p$; e, visto que, de 1 até M, há tantos números que são primos com M, quantas unidades são contidas em m, esses, sejam eles primos, ou compostos de primos, são maiores[11] que p.

137. Se, de 1 até M, houver m números primos com M, haverá, de 1 até $2M$, $2m$ números primos com M e, em geral, haverá, de 1 até NM, Nm números primos com M. Então, em qualquer intervalo,

$$1 \ldots M, \quad M+1 \ldots 2M, \quad 2M+1 \ldots 3M, \quad 3M+1 \ldots 4M, \textit{ etc}.$$

a quantidade de números primos com M é a mesma.

138. Se N designar um número qualquer e se de 1 até N houver n números primos com N, então de 1 até MN haverá Mn números primos com N. E no mesmo intervalo há Nm números primos com M. Mas os que são primos com MN, são os que são primos tanto com M, quanto com N.

---

[10] N. do Trad. Ver §132.

[11] N. do Trad. Se x é um número primo, que é primo com M, x não é contido em M. Mas, M é o produto de todos os números primos de 2 a p. Portanto, $x > p$.

139. Antes, porém, mostramos[12] que, se os números *M* e *N* forem primos entre si, então haverá no intervalo 1 ... *MN* tantos números primos com *MN*, quantas unidades são contidas em *mn*; e esses números ocorrerão em cada um dos referidos agregados, *Mn* e *Nm*. (*)

(*) *Notas do ilustre autor acrescentadas na margem*. Sobre o máximo divisor comum e como achá-lo. – Se *A* e *B* são número primos, um múltiplo de *A* pode ser achado, que, dividido por *B*, deixa um dado número *C* como resto. – Se os números forem primos entre si, quaisquer potências deles serão primos entre si. – Se *A* for primo com *B*, bem como com *C*, então também será primo com *BC*. – Se o produto *AB* for divisível pelo primo *p*, um dos dois fatores será divisível por ele. – Se *A* e *B* forem primos entre si, poderão ser achados números *m* e *n*, tais que fazem $mA-nB = 1$, ou qualquer outro número dado. – Se φ for o máximo fator comum dos números *A* e *B*, então $\frac{A}{\varphi}$ e $\frac{B}{\varphi}$ serão primos entre si. – Se *a*, dividido por *b*, deixar o resíduo *r*, então *na*

[12] N. do Trad. Ver §133.

dividido por nb deixará o resíduo nr. – Se a, dividido por b, deixar o resíduo r, um fator comum dos números a e b, se tiveram algum além da unidade, também será um fator do resíduo r. – Por sua vez, se b e r tiveram um fator comum, o mesmo também será um fator do próprio a. – Se a e b forem números primos entre si com $a > b$, teremos $a = mb+p$; mas $b > p$, assim, $b = np+q$ com $p > q$ e assim por diante até chegamos à unidade.

Capítulo V

Sobre resíduos surgidos por divisão

140. Se o número a não for um múltiplo do número b, o primeiro não é divisível pelo segundo e o excesso do número a sobre o maior múltiplo de b menor que a é chamado o *resíduo* resultando da divisão. Assim, se tivermos $a = mb+r$, r será o resíduo surgido da divisão do número a por b.

141. Disto, fica claro que o resíduo r sempre é menor que o número b, ou seja, o divisor; pois, se fosse igual, isto é, $r = b$, ao aumentar o índice da multiplicação, m, por uma unidade, a seria um múltiplo de b, ou seja, $a = (m+1)b$; e se tivéssemos $r > b$, ao aumentar o índice m, o resíduo seria reduzido abaixo de b.

142. Seja proposto, então, qualquer b como divisor; se o dividendo a for um múltiplo desse b, o resíduo será = 0. Se, porém, a não for um múltiplo de b, o resíduo será ou 1, ou 2, ou 3, ou algum outro número menor que b. Em consequência, a quantidade de resíduos que podem surgir é b–1, ou ainda será b se o zero for contado.

143. Em relação a qualquer divisor b, portanto, todos os números podem ser distribuídos em tantas classes, quantas unidades são contidas em b. A primeira classe conterá, de fato, todos os números que são múltiplos de b, ou seja, os da forma

mb; a segunda, os que, quando divididos por *b*, deixam o resíduo 1; a terceira, os que deixam 2; a quarta, os que deixam 3; até, finalmente, a última, os que deixam *b*–1.

144. Assim, tomando 2 como o divisor, há duas classes, das quais a primeira contém números da forma 2*m*, enquanto a segunda contém números da forma 2*m*+1. Os números da primeira classe são chamados *pares* e os da segunda *ímpares*.

145. Se tomarmos três como o divisor, todos os números serão separados em três classes: a primeira consistirá de números da forma 3*m*, a segunda de números da forma 3*m*+1 e a terceira de números da forma 3*m*+2.

146. Se o divisor for = 4, as quatro classes de todos os números terão as seguintes quatro formas: I. 4*m*. II. 4*m*+1, III. 4*m*+2, IV. 4*m*+3, onde os números da primeira classe são *parmente pares*,[1] enquanto os da terceira classe são *imparmente pares*. A segunda e quarta mostram os números ímpares subdivididos em duas classes.

147. De modo semelhante, o divisor 5 fornece as seguintes cinco classes de números: I. 5*m*, II. 5*m*+1, III. 5*m*+2, IV. 5*m*+3, V. 5*m*+4. O divisor 6 dá as seguintes seis classes:

I. 6*m*, II. 6*m*+1, III. 6*m*+2, IV. 6*m*+3, V. 6*m*+4, VI. 6*m*+5,

e assim por diante para qualquer outro divisor.

[1] N. do Trad. Ver §109.

148. Assim, todo número pertencerá a alguma determinada classe, ou seja, tomará alguma determinada forma, com respeito a qualquer divisor; isto pode ser feito em um número infinito de maneiras, pois o número de divisores é infinito.

149. Se, por exemplo, um número for menor que o divisor proposto, o próprio número pode ser considerado o resíduo, sendo desvanecido o índice do múltiplo. Isto é, se tivermos $a < b$, então teremos $a = mb+a$, sendo $m = 0$. O número 3, portanto, com respeito ao divisor 5, pertence à classe $5m+3$.

150. Uma classe qualquer é composta de infinitos números crescendo em progressão aritmética, sendo a diferença entre dois consecutivos igual ao divisor. Assim, em geral, se o divisor é b e o resíduo r, todos os números da classe $mb+r$ são exprimidos assim: r, $b+r$, $2b+r$, $3b+r$, $4b+r$, $5b+r$, *etc*. O termo geral dessa progressão aritmética é a própria fórmula $mb+r$, da qual ela surge.

151. A fórmula $mb+r$ pode, de fato, ser representada assim: $(m+1)b–b+r$. Desta forma, o resíduo positivo r deve ser julgado equivalente a um resíduo negativo, $–(b–r)$; disto, fica claro que a ideia de resíduos se amplia para compreender os números negativos.

152. Desta forma, send'o o divisor $b = 2$, a fórmula para os números ímpares, $2m+1$, também pode ser representada como $2m-1$; e se o divisor b é = 3, a classe de números que deixam 2, quando divididos por 3, é também definida pela fórmula $3m-1$. Assim, todo número é necessariamente contido em uma das três classes $3m$, $3m+1$ e $3m-1$.

153. Por isto, se pretendermos admitir resíduos negativos, poderemos representar todas as fórmulas $mb \pm r$ de tal forma que o resíduo r não excede a metade do divisor b. Pois, se tivermos $r > \frac{1}{2}b$, tomaremos $-(b-r)$ para r e obteremos $b-r < \frac{1}{2}b$.

154. De modo semelhante, visto que $mb+r = (m-1)b+b+r$, o resíduo r é equivalente ao resíduo, tomando esse palavra num sentido lato, $b+r$. Em geral, portanto, os resíduos (ainda usando a palavra nesse sentido lato) $b+r$, $2b+r$, $3b+r$, *etc*. são equivalentes ao resíduo propriamente dito, r.

155. Sem dúvida, então, sendo b o divisor, todo número, mesmo que seja maior que b, pode ser considerado um resíduo, que será reduzido ao resíduo propriamente dito, subtraendo o divisor b quantas vezes forem necessárias, e, admitindo valores negativos, pode até ser reduzido abaixo da metade do próprio b.

156. Assim, sejam o divisor 6 e o resíduo 16. Então esse resíduo impróprio será reduzido ao resíduo próprio 4, ou até ao

resíduo negativo –2, o que é o mesmo de tomar como equivalentes as fórmulas $6m+16$, $6m+4$ e $6m-2$, pois todo número contido em uma é também contido nas outras.

157. Convém considerar mais propriedades notáveis sobre resíduos. Se o número A, dividido por d, fornecer o resíduo α, também os números $A+d$, $A+2d$, $A+3d$, *etc*., deixarão o mesmo resíduo α. Mas, o número $A+1$, dividido por d, dará o resíduo $\alpha+1$ e, em geral, o número $A+n$ dará o resíduo $\alpha+n$, que, se isto exceder o divisor, será reduzido à forma mínima, por subtrair d quantas vezes forem necessárias.

158. De modo semelhante, se, tomando d como o divisor, o número A produzir o resíduo α, também os números $A-d$, $A-2d$, $A-3d$, *etc*., deixarão o mesmo resíduo; mas, o número $A-1$ produzirá o resíduo $\alpha-1$ e o número $A-n$, o resíduo $\alpha-n$, que, se isto for por acaso negativa, será reduzido a um positivo por somar o divisor d.

159. Tomando d como o divisor, se o número A fornecer o resíduo α e o número B o resíduo β, a soma desses números $A+B$ deixará o resíduo $\alpha+\beta$, que é congruente[2] ao $\alpha+\beta-d$, se, por

[2] Para descrever essa relação, Euler usa palavras que significam, no fundo, concordância entre os números ou que são agradáveis umas aos outras. Aqui pela primeira vez usa uma forma de "congruente" (*congruere*, ao pé de letra "correr juntos"), que viria a ser o termo técnico para a referida relação.

acaso, $\alpha+\beta > d$. Disto, fica claro que, se tivermos $\alpha+\beta = d$, então $A+B$ será um múltiplo do próprio d.

160. Dadas as mesmas convenções, a diferença dos referidos números, $A–B$, deixará o resíduo $\alpha–\beta$, ou $\alpha–\beta+d$, se, por acaso, $\beta > \alpha$. Em consequência, se tivermos $\alpha = \beta$, ou seja, se os números A e B deixarem resíduos iguais, então sua diferença será divisível pelo divisor d.

161. Tomando d como o divisor, se o número A fornecer o resíduo α, seu duplo $2A$ dará 2α como resíduo, ou então $2\alpha–d$; seu triplo $3A$ dará 3α como resíduo, cuja forma mínima, se o mesmo for maior que d, será ou $3\alpha–d$, ou $3\alpha–2d$. E, em geral, o resíduo de um múltiplo qualquer nA será $n\alpha$, ou seja, $n\alpha–md$.

162. Seja o divisor proposto $= d$. Se o número A corresponder ao resíduo α e o número B ao resíduo β, o produto AB produzirá o resíduo $\alpha\beta$, o qual, se, por acaso, for maior que o divisor d, será reduzido para $\alpha\beta–d$, ou $\alpha\beta–md$.

163. Pois, teremos $A = md+\alpha$ e $B = nd+\beta$, o que faz com que o produto seja

$$AB = mnd^2+(m\beta+n\alpha)d+\alpha\beta$$

e, como suas primeiras partes são divisíveis por d, a última parte, $\alpha\beta$, pode ser considerada o resíduo.

164. Disto, concluímos que, se o número A, quando divido por d, deixar o resíduo α, seu quadrado A^2 corresponderá ao resíduo α^2, seu cubo A^3, ao resíduo α^3, e uma potência qualquer A^n, ao resíduo α^n, o que, feita a divisão por d, será reduzido, por sua vez, à forma mínima.

165. Em consequência, se o número A, quando dividido por d, deixar um resíduo = 1, todas as suas potências A^2, A^3, A^4, *etc*., quando divididas pelo mesmo d, também deixarão resíduo = 1. Mas, se o resíduo do número A for -1, que é equivalente a $d-1$, as potências pares A^2, A^4, A^6, A^8, *etc*., terão +1 como resíduo, enquanto as ímpares terão -1.

166. Finalmente, deve ser observado que, se o número A, dividido por d, fornecer o resíduo α, então $A-\alpha$ será divisível por d. Daí, visto que A^n, dividido por d, dá o resíduo α^n, também $A^n-\alpha^n$ será divisível por d.

Capítulo VI

Sobre resíduos surgidos da divisão de termos em progressão aritmética

167. Vamos começar por dividir a sequência dos números naturais, cujos termos são 1, 2, 3, 4, *etc*., por um divisor qualquer d. Obtemos os resíduos 1, 2, 3, 4, *etc*., até chegamos ao termo d, cujo resíduo é = 0; os termos seguintes, $d+1$, $d+2$, $d+3$, *etc*., repetem os resíduos 1, 2, 3, *etc*., na mesma ordem, até $2d$, cujo resíduo se anula de novo, e assim por diante.

168. Agora, seja proposta uma progressão aritmética qualquer

$$a,\ a+b,\ a+2b,\ a+3b,\ a+4b,\ a+5b,\ etc.,$$

cujos termos devem ser divididos pelo divisor d. E seja a o resíduo do primeiro termo, que só ocorrerá de novo quando chegarmos ao termo $a+nb$, sendo a parte nb divisível por d. Em seguida, os resíduos dos termos serão repetidos na mesma ordem como do início. (*)

* *Escrito na margem*. Esses resíduos excedem pelo número a os resíduos surgidos da progressão 0, b, $2b$, $3b$, $4b$, *etc*.; consequentemente basta desenvolver essa progressão.

169. Será imediatamente claro, em primeiro lugar, que não é possível ter mais resíduos distintos do que o número de unidades contidas no divisor d. Em consequência, se, do início até um certo ponto, esse tanto de resíduos diferentes foram produzidos, é necessário que esses se repitam subsequentemente. Ainda mais, o termo $a+db$, cujo índice[1] é $d+1$, sempre fornecerá o mesmo resíduo que o primeiro termo, a.

170. Se a diferença b da progressão for fator do divisor d, ou se b e d tiveram pelo menos um fator comum φ, de modo que $b = B\varphi$ e $d = D\varphi$, então, antes de chegar ao termo $a+db$, o primeiro resíduo a será repetido; isto acontece, decerto, para o termo $a+Db$ (cujo índice é $D+1$), pois $Db = BD\varphi = Bd$ é divisível por d.

171. Assim, convém distinguir dois casos: um, em que o divisor d e a diferença[2] b da progressão são números primos entre si, o outro, em que são números compostos entre si, isto é, eles têm algum fator comum além da unidade.

172. Se o divisor d e a diferença b da progressão forem primos entre si, o primeiro resíduo a não será repetido antes do

[1] N. do Trad. Aqui o *índice* indica a posição do elemento dentro da progressão. Assim, $a+db$ é o $(d+1)$-ésimo termo da progressão a, $a+b$, $a+2b$, ...

[2] N. do Trad. O texto original tem "e a diferença a". Na tradução, porém, mantivemos a notação estabelecida nos parágrafos anteriores.

termo $a+bd$; pois, se fosse repetido para um determinado termo anterior, digamos $a+(d-n)b$, então $(d-n)b$ e, logo, nb, seria divisível por d, e, portanto, também[3] n, o que é absurdo.

173. Para determinar os resíduos, portanto, deve-se considerar os termos da progressão do primeiro, a, até $a+(d-1)b$; teremos então d termos, que podem ser representados, dispostos em ordem, com seus resíduos, da seguinte maneira[4]:

Índices:	1,	2,	3,	4,	5,	d
Progressão:	a,	$a+b$,	$a+2b$,	$a+3b$,	$a+4b$, ...	$a+(d-1)b$
Resíduos:	α,	β,	γ,	δ,	ε,	λ

174. Primeiro, então, observamos que esses resíduos, cuja quantidade é $= d$, são todos distintos. Pois, do mesmo modo em que foi mostrado[5] que o primeiro, α, não ocorre mais do que uma vez, mostra-se que o segundo β está presente somente uma vez. Pois, se o mesmo resíduo surgisse no termo $a+nb$, onde $n < d$, a diferença $(n-1)b$ dos termos e, portanto, $n-1$ seriam divisíveis por d, o que é absurdo.

175. Visto, então, que todos os resíduos $\alpha, \beta, \gamma, \delta, \varepsilon, ..., \lambda$ são distintos e que sua quantidade é $= d$, todos os números menores que d, incluindo o zero, ocorrem entre os resíduos, isto é, os números 0, 1, 2, 3, ..., $(d-1)$ ocorrem, e sua quantidade é justamente $= d$.

---

[3] N. do Trad. Isto é, n também seria divisível por d, mas, por hipótese, $0 < n < d$.

[4] N. do Trad. No presente parágrafo Euler generaliza pela primeira vez, adotando o símbolo α para o resíduo de a. Claramente, $\alpha = a$, sempre que $0 \leq a < d$ e, senão, $\alpha \equiv a \pmod{d}$.

[5] N. do Trad. Em §172.

176. Para essa razão, se r for um número qualquer, menor que o divisor d, então certamente terá um termo da progressão, $a+nb$, sendo $n < d$, o qual, quando dividido por d, deixa o resíduo r. Ainda mais, tomando $r = 0$, haverá algum termo, $a+nb$, do referido tipo, que é divisível por d.

177. Se o termo $a+nd$ fornecer o resíduo r, então $a+nb–r$ será divisível por d. Assim, se b e d são números primos entre si e $a–r$ denotar um número qualquer, sempre terá um número n, menor que d, tal que o número $a–r+nb$ seja divisível por d.

178. Seja $a+mb$, com $m < d$, o termo divisível por d. Então, o termo seguinte, $a+(m+1)b$, terá b como resíduo e o precedente, $a+(m–1)b$, terá $–b$, ou, $d–b$. Seja, em seguida, o termo $a+nb$ o que, quando dividido por d, deixa a unidade. Então, o número $(n–m)b$, obtido pela diferença entre esses, também deixa a unidade.[6]

179. Ponhamos $n–m = p$, de tal forma que o número pb, divido por d, deixa a unidade, onde o termo $a+mb$ é o termo que é divisível por d. Assim, o termo $a+(m+p)b$ deixa resíduo = 1, o termo $a+(m+2p)b$, resíduo = 2, o termo $a+(m+3p)b$, resíduo = 3 e, em geral, o termo $a+(m+np)b$, resíduo = n.

[6] N. do Trad. Ver §159 e §160.

180. Se $m+np$ for maior que o divisor d, isto será subtraído tantas vezes até chegar a um número $k < d$; o termo $a+kb$, dividido por d, deixará resíduo $= n$.

181. Assim, será bastante fácil determinar os termos que deixam um dado resíduo, uma vez que o produto pb, que deixa a unidade quando dividido por d, for conhecido. Como o primeiro termo a deixa o resíduo α, o termo $a+npb$ deixa o resíduo $\alpha+n$.

182. Se, portanto, o dado resíduo for $= r$, ponhamos $\alpha+n = r$, e, visto que $n = r-\alpha$, sendo p conhecido, o termo fornecendo o resíduo r será $a+(r-\alpha)pb$; ou, de forma mais geral, $a+((r-\alpha)p\pm\mu d)b$, onde μ pode ser tomado de tal forma a fazer $(r-\alpha)p\pm\mu d < d$.

183. Tudo é, portanto, reduzido a achar um múltiplo pb do número b, que, quando dividido por d, deixa a unidade como resíduo. Como $pb-1$ é divisível por d, pomos $pb-1 = qd$ e procuramos números p e q que satisfazem[7] a equação $pb-qd = 1$. Ainda mais, sempre podemos fazer p menor que d.

184. É frequentemente mais fácil achar um produto πb que, quando dividido por d, deixa resíduo $d-1$, ou seja, -1; então o produto $(d-\pi)b$ fornecerá o resíduo $= +1$ e, como π é conhecido, devemos fazer $p = d-\pi$. Então, o termo $a+((\alpha-r)\pi\pm\mu d)b$ deixará r, o resíduo procurado.

[7] N. do Trad. Isto é sempre possível, como Euler observou nas notas (*) depois de §139. Observe também que, se $p > d$, pomos, como sempre $p' = p-kd$; então, para $q' = q-kb$, teremos $p'b-q'd = pb-qd = 1$, com $p' < d$.

185. Consideremos agora resíduos que surgem quando a diferença b da progressão e o divisor d não são números primos inter si. Como já vimos[8], se o fator comum seja φ, de tal modo que $b = B\varphi$ e $d = D\varphi$, o termo $a+Db$ fornece o mesmo resíduo que o primeiro, a.

186. Para essa razão, se φ for o máximo fator comum dos números b e d, visto que o primeiro resíduo a, ou α, aparecerá de novo no termo $a+Db$, só terá lugar para D resíduos distintos; assim, nem todos os números menores que o divisor d ocorrerão entre os resíduos.

187. Para examinar esses resíduos de forma mais fácil, pomos $a = 0$. Os termos da progressão, com seus resíduos serão:

Índices:	1	2	3	4	D
Termos:	0,	$B\varphi$,	$2B\varphi$,	$3B\varphi$, ...,	$(D-1)B\varphi$
Resíduos:	0,	$\beta\varphi$,	$\gamma\varphi$,	$\delta\varphi$,	$\lambda\varphi$

e é claro que, se esses termos forem divididos por $d = D\varphi$, os resíduos serão divisíveis por φ.

188. Pois, se mB fornecer o resíduo r quando dividido por D, teremos $mB = nD+r$ e, assim, $mB\varphi = nD\varphi+r\varphi$. Em consequência, se $mB\varphi$ for dividido por $D\varphi = d$, o resíduo será $r\varphi$, um múltiplo do próprio φ. Portanto, como todos os números

[8] N. do Trad. Em §170.

menores que D são produzidos[9] para r, e como todos os múltiplos de φ, que não superam o divisor $d = D\varphi$, devem ocorrer entre esses resíduos, sua quantidade é certamente $= D$.

189. Se somarmos a cada termo o número a, seus diversos resíduos serão aumentados pela mesma quantidade; assim, sendo $b = B\varphi$ e $d = D\varphi$, teremos:

Índices:	1	2	3	4	5	D
Termos:	a,	$a+b$,	$a+2b$,	$a+3b$,	$a+4b$, ...,	$a+(D-1)b$
Resíduos:	a,	$a+\beta\varphi$,	$a+\gamma\varphi$,	$a+\delta\varphi$,	$a+\varepsilon\varphi$,	$a+\lambda\varphi$

onde a sequência β, γ, δ, ε, ..., λ contém todos os números menores que D.

190. Nesse caso, portanto, serão excluídos da sequência de resíduos todos os números, que, diminuídos por a, não são divisíveis por φ (o máximo divisor comum entre a diferença b e o divisor d).

191. Como os números B e D são primos entre si, podemos achar um múltiplo do primeiro, digamos mB, tal que, quando dividido por D, deixa um dado resíduo r. Desta forma, o termo $a+mB\varphi$ da nossa progressão, ou seja, o termo $a+mb$, dividido por $D\varphi = d$, deixa o resíduo $a+r\varphi$. (*)

(*) *Escrito na margem*: Método de determinar uma fórmula $ax+b$ que seja divisível pelo dado número d.

[9] N. do Trad. Observe que B e D são primos entre si.

Capítulo VII

Sobre resíduos surgidos da divisão de termos em progressão geométrica

192. Em geral, representamos uma progressão geométrica assim: a, ab, ab^2, ab^3, ab^4, ab^5, *etc*. Quando os referidos termos são divididos por um número d qualquer, deixando resíduos, é fácil calcular os mesmos dos resíduos da progressão 1, b, b^2, b^3, *etc*., multiplicando estes por a.

193. Assim, estamos conduzidos a uma investigação de resíduos de potências puras, isto é, queremos determinar o resíduo deixado por um potência qualquer b^n, quando dividido por um dado número d. Aqui, de fato, convém distinguir dois casos, os em que os números b e d são ou primos, ou compostos, entre si.

194. Sejam $b = p\varphi$ e $d = q\varphi$ e vamos procurar o resíduo que surge de $p^n\varphi^{n-1}$, quando divido por q. O mesmo, multiplicado por φ, dará o resíduo que surge da divisão do número $p^n\varphi^n$ por $q\varphi$ e, desse modo, o problema é reduzido à divisão da potência b^n por d, onde b e d são primos entre si.

195. Sejam, então, b e d números primos entre si; os resíduos resultando da divisão das potências de b são indicados da seguinte maneira:

Potências: $1,\ b,\ b^2,\ b^3,\ b^4,\ b^5,\ b^6,\ b^7,$ *etc*.
Resíduos: $1, \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,$ *etc*.,

todos dos quais serão também primos com o divisor[1] d, pois d é primo com todas as potências de b.

196. Visto que todos os referidos resíduos $1, \alpha, \beta, \gamma, \delta,$ *etc*. são menores que d, todos não podem ser distintos. Na verdade, se μ seja a quantidade de números que são primos com d e também menores que ele, não é possível ter mais resíduos distintos que μ contém de unidades. [2]

197. Portanto, como há infinitas[3] potências que fornecem o mesmo resíduo, supondo que b^m e b^{m+n} dão o mesmo resíduo, a diferença entre essas duas potências $b^{m+n}-b^m = b^m(b^n-1)$ será divisível por d. Mas, visto que b^m é primo com d, segue que b^n-1 é divisível por d, ou seja, a potência b^n dá resíduo = 1.

198. Porque não poder haver mais do que μ resíduos distintos, se a progressão for continuada até o termo b^μ, o qual é o termo de número = $\mu+1$, pelo menos um resíduo ocorrerá duas vezes e, como aconteceu no caso anterior, antes que $m+n$ supera

[1] N. do Trad. Seja $b^n = qd+r$. Se $a \mid d$ e $a \mid r$, então $a \mid qd+r$, ou seja $a \mid b^n$, o que contradiz a hipótese de que $(b, d) = 1$ (ver §164).
[2] N. do Trad. Visto que os resíduos têm de ser primos com o divisor d (§95).
[3] N. do Trad. Há um número infinito de potências b^k, mas apenas um número finito (d) de resíduos. Portanto, pelo menos um resíduo deve ocorrer um número infinito de vezes.

μ, chegamos[4] a um ponto em que a potência b^n dará o resíduo = 1, de modo que n não supera μ.

199. Seja b^n o menor, depois da própria unidade, potência que deixa a unidade quando dividida por d. Então as próximas potências, b^{n+1}, b^{n+2}, b^{n+3}, *etc*., fornecerão os mesmos resíduos que as potências iniciais, b, b^2, b^3, *etc*., até chegamos à potencia b^{2n}, que deixará, mais uma vez, a unidade como resíduo.

200. Como, ao percorrer do início por passos de b^n, os mesmos resíduos se repetem, não somente acontece que todas as potências b^0, b^n, b^{2n}, b^{3n}, b^{4n}, *etc*. deixam o mesmo resíduo 1, mas também b^1, b^{n+1}, b^{2n+1}, b^{3n+1}, b^{4n+1}, *etc*., têm os mesmos resíduos e, ainda mais, b^m, b^{n+m}, b^{2n+m}, b^{3n+m}, *etc*., deixam resíduos iguais quando divididas por d.

201. Pondo, então, b^n para a menor potência que deixa a unidade como resíduo, de modo que n não excede μ, a quantidade de números menores que o próprio d e primos com ele, todas as potências precedentes, 1, b, b^2, b^3, ..., b^{n-1}, fornecerão resíduos distintos, que se repetem em seguida na

[4] N. do Trad. O texto não é inteiramente claro, mas o sentido parece ser algo como o seguinte. Seja r o resíduo do termo b^μ; visto que esse resíduo é repetido, r é também o resíduo de algum termo anterior, b^m. Pondo $\mu = m+n$ o resíduo de b^n é 1 (pelo argumento do parágrafo anterior) e n claramente não é maior que μ. Observe que, embora o resíduo de b^μ seja necessariamente repetido, não é necessariamente o *primeiro* resíduo repetido.

mesma ordem. Pois, se dois deles fossem iguais, teríamos um valor menor para n, contra a hipótese.

202. Quando, portanto, todos os números que são primos com o divisor d e menores que ele, cuja quantidade é μ, ocorrerem entre os resíduos, teremos $n = \mu$ e $b^{\mu}-1$ será divisível por d. No entanto, se nem todos os números que são primos com d ocorrerem entre os resíduos, será necessário que seja $n < \mu$. Mostraremos que, neste caso, n é uma parte alíquota de μ.

203. Se nem todos os números que são primos com d e menores que ele, cuja quantidade é $= \mu$, ocorrerem entre os resíduos, cuja quantidade é $= n$, chamarei os, que são excluídos da classe dos resíduos, pelo nome de *não-resíduos* e, assim, a quantidade de resíduos n, junto com a quantidade de não-resíduos, devem exaurir o número μ.

204. Se os números r e s ocorrerem na sequência de resíduos $1, \alpha, \beta, \gamma$, *etc*., o número rs também nela ocorrerá, ou seja, o resíduo correspondendo ao mesmo. Pois[5], se os resíduos r e s corresponderem às potências b^{ρ} e b^{σ}, o resíduo rs corresponderá à potência $b^{\rho+\sigma}$. Assim, o número $r^f s^g$ ocorrerá entre os resíduos, qualquer que seja a maneira em que os expoentes f e g são tomados.

[5] N. do Trad. Ver §159. Em geral, a aritmética elementar de resíduos é abordada em Capítulo 5.

205. Por sua vez, se a potência b^{ρ} fornecer o resíduo r e a potência $b^{\rho+\sigma}$ o resíduo rs, ou $rs-\lambda d$, então a potência b^{σ} produzirá o resíduo s. Pois, o produto $b^{\rho}s$ produzirá o resíduo rs, o mesmo que a potência $b^{\rho+\sigma}$; desta forma, a diferença $b^{\rho+\sigma}-b^{\rho}s = b^{\rho}(b^{\sigma}-s)$ será divisível por d. Em consequência, visto que b^{ρ} é primo com d, é necessário que $b^{\sigma}-s$ seja divisível por d e, assim, a potência b^{σ} corresponde ao resíduo s.

206. Se, portanto, os números r e rs são achados entre os resíduos, é certo que o número s também será achado entre eles. Mas, se a sequência dos resíduos 1, α, β, γ, δ, *etc*., cuja quantidade é = n, não completar todos os números menores que d e primos com ele, cuja quantidade é = μ, haverá um deles, ou talvez mais, que deve pertencer à classe dos não-resíduos.

207. Seja x um não-resíduo; então é claro que os números αx, βx, γx, δx, *etc*., serão achados entre os não-resíduos, pois se αx fosse achado entre os resíduos, visto que α está entre eles, x também deveria ser achado entre os mesmos, contra a hipótese. Da existência de um único não-resíduo, portanto, segue necessariamente que existem tantos não-resíduos quantos resíduos[6], a saber, n. Pois esses não-resíduos são todos

[6] N. do Trad. Como será evidente a partir dos próximos parágrafos, não devemos conceber isto como afirmando que há *exatamente* tantos não-resíduos quanto resíduos, mas que há *pelo menos* tantos não-resíduos quanto resíduos.

distintos, exatamente como os resíduos 1, α, β, γ, δ, *etc*.; se houvesse dois daqueles iguais, então haveria dois destes iguais[7], o que é absurdo. (*)

(*) *Escrito na margem*: Sejam x e y não-resíduos. Então, $y = \alpha x$ e $xy = \alpha xx$; se o número de não-resíduos = o número de resíduos, deve ser demonstrado que xx é contido entre os resíduos.

208. Seguramente, portanto, $n < \mu$ e há no mínimo n não-resíduos; quando esses completar o todo, haverá tantos não-resíduos quanto resíduos[8], numerando $n+n$, que é igual a μ. Em consequência, $n = \frac{\mu}{2}$; assim, se $n < \mu$, não é possível que n supera metade do número μ.

209. Se nem todos os não-resíduos ocorrerem entre os já exibidos, x, αx, βx, γx, *etc*., seja y um número $< d$ e primo com ele, que não é achado entre esses não-resíduos, nem entre os resíduos. Então, de forma semelhante, os números αy, βy, γy, *etc*., que são diferentes dos precedentes[9], devem pertencer aos não-resíduos, e assim, teremos mais n não-resíduos.

[7] N. do Trad. Claramente 0 não pode ser um resíduo, pois, senão, teríamos $d|b^k$, para algum k.

[8] N. do Trad. Aqui há *exatamente* tantos não-resíduos quanto resíduos.

[9] N. do Trad. Como Euler mencionará em §242, cada resíduo tem uma inversa entre os resíduos. É fácil ver isto, pois os n produtos $\alpha\alpha$, $\alpha\beta$, $\alpha\gamma$, *etc*. são todos distintos (e 1 sempre é um resíduo); portanto, um destes é 1. Assim, se $\alpha y = \beta x$, ao multiplicar pela inversa, teremos $y = \gamma x$, para algum resíduo γ, contra a hipótese.

210. Se esses dois tipos ainda não exaurirem todos os não-resíduos, haverá outro tipo, igualmente contendo n termos, ou talvez ainda mais contendo o mesmo número de termos; desta forma, concluímos que o número de todos os não-resíduos, a não ser que não houver qualquer um, será igual ou a n, ou seu duplo, ou seu triplo, ou, em geral, um múltiplo qualquer.

211. Como, então, todos os não-resíduos, juntos com os resíduos, devem exaurir a quantidade de todos os números menores que o divisor d e primo com ele, teremos ou que $n = \mu$, ou $2n = \mu$, ou $3n = \mu$, *etc*., de tal forma que o expoente[10] n é sempre uma parte alíquota do número μ.

212. Mas, se b e d forem números primos entre si, e μ denotar a quantidade de todos os números que são primos com d e menores que ele e, ainda, b^n for a mínima potência, depois do caso $n = 0$, que, dividido por d, deixa a unidade, então teremos que ou $n = \mu$, ou n será igual a alguma parte alíquota de μ, de tal forma que teremos $n = \frac{\mu}{m}$, sendo m algum divisor do próprio μ.

213. Como se sabe[11] que, além da potência b^n, todos esses b^{2n}, b^{3n}, b^{4n}, *etc*. têm a unidade como resíduo, a potência

[10] N. do Trad. Isto é, fator.
[11] N. do Trad. Ver §199 e §200.

$b^{mn} = b^{\mu}$ sempre deixará a unidade quando dividido por d. Daí,[12] quando b e d forem números primos entre si, a fórmula $b^{\mu}-1$ sempre será divisível pelo número d.

214. Ainda mais, se c e d forem números primos entre si, visto que $c^{\mu}-1$ admite a divisão por d, a diferença entre essas fórmulas, $b^{\mu}-c^{\mu}$, sempre será divisível pelo número d, uma vez que cada um dos números b e c seja primo com d.

215. Se tomarmos para d o número primo p, teremos $\mu = p-1$ e, então, a fórmula $b^{p-1}-1$ sempre será divisível por p, exceto quando o número b for um múltiplo do próprio p. Também pode acontecer, no entanto, que a forma mais simples b^{n-1} admite a divisão por p, onde, porém, é necessário requerer que o expoente n seja uma parte alíquota de $p-1$.

216. Se o divisor for $d = pq$, sendo p e q números primos distintos e b não conter esses números, então, porque $\mu = (p-1)(q-1)$, a fórmula $b^{(p-1)(q-1)}-1$ será divisível por d.

217. E, sendo p, q, r, s, números primos distintos, se tivermos $d = p^{\lambda}q^{\mu}r^{\nu}s^{\xi}$, com b um número qualquer primo com d, posto que

$$m = p^{\lambda-1}(p-1)q^{\mu-1}(q-1)r^{\nu-1}(r-1)s^{\xi-1}(s-1),$$

[12] N. do Trad. Este resultado é chamado, hoje em dia, o Teorema de Euler; é uma generalização do Pequeno Teorema de Fermat: para p primo, p divide a^p-a.

a forma b^m–1 sempre será divisível por d; às vezes, pode acontecer que uma fórmula mais simples b^n–1, sendo n alguma parte alíquota do próprio m, será divisível.[13]

218. Mas, vamos voltar para o divisor geral d, e seja μ a quantidade de números menores que d e primos com ele; ainda mais, tomemos por b um número qualquer primo com d, e seja b^n a menor potência do mesmo que, dividido por d, deixa a unidade. Vimos, então, que é necessário que ou $n = \mu$, ou $n = \frac{1}{2}\mu$, ou $n = \frac{1}{3}\mu$, ou $n = \frac{1}{4}\mu$, ou $n = \frac{1}{5}\mu$, uma vez que μ admita tais partes alíquotas. Convém investigar esses casos com mais cuidado.

219. Poderemos até conjeturar que esses casos dependam da natureza do número b, de tal forma que, para um dado divisor d, certos números tomados por b fornecerão $n = \mu$, outros $n = \frac{1}{2}\mu$, outros $n = \frac{1}{3}\mu$, outros $n = \frac{1}{4}\mu$, ou até partes alíquotas ainda menores de μ.

220. Ora, seja n qualquer parte alíquota de μ; se as duas potências b^n e e^n deixarem a unidade, então sua composta $(be)^n$ deixará a unidade. Ainda mais, é claro que a potência $(b \pm \lambda d)^n$, dividida por d, deixará a unidade.

[13] N. do Trad. Observe que nesse parágrafo, Euler usa m no lugar de μ, pois μ é usado como um dos expoentes.

221. Como a potência b^{μ} sempre deixa a unidade, procuramos números, tomados para b, para os quais $b^{\frac{1}{2}\mu}$ deixa a unidade, em qual caso é necessário, antes de tudo, que μ seja um número par, que de fato sempre acontece exceto quando $d = 2$.

222. Se tomarmos $b = ee$, onde e seja primo com d, é certo que $b^{\frac{1}{2}\mu} = e^{\mu}$ deixa a unidade, que também acontece quando $b = ee \pm \lambda d$. Números menores[14], a serem tomados por b, portanto, são resíduos que resultam da divisão de números quadrados por d, sob a condição que o quadrado seja primo com d.

223. De modo semelhante, a potência $b^{\frac{1}{3}\mu}$, dividida por d, deixará a unidade, se tivermos $b = e^3$ ou, em geral, se $b = e^3 \pm \lambda d$. Portanto, valores menores apropriados de b são resíduos, que surgem da divisão por d de cubos, primos com d. É evidente, no entanto, que isto não pode acontecer, a não ser que μ seja divisível por 3.

[14] N. do Trad. A redação de Euler neste, e nos próximos três, parágrafos não parece muito feliz. Em §219, ele conjecturou que, para qualquer parte alíquota ν de μ, haverá algum b tal que b^{ν} deixa a unidade quando dividido por d (ou seja, $b^{\nu} \equiv 1 \pmod{d}$). Nos referidos parágrafos, exibiu um procedimento que comprova a conjectura. Exemplificamos com $d = 9$ (ver §233). Então, $\mu = 6$ e, em consequência, $5^6 \equiv 1 \pmod{9}$. Mas, $\mu = 2 \times 3$ e, assim, consideramos que 5^2 e 5^3, que deixam restos de 7 e 8. Mas, de fato, 7^3 e 8^2 deixam a unidade como resto quando dividido por 9 (ou seja, $7^3 \equiv 1$ e $8^2 \equiv 1 \pmod{9}$). Observe que, 4^6 também deixa a unidade como resto quando dividido por 9; fazendo 4^3, achamos que isto já deixa a unidade sob as referidas condições (ou seja, $4^6 \equiv 4^3 \equiv 1 \pmod{9}$).

224. Seja μ divisível por 4. Então a potência $b^{\frac{1}{4}\mu}$, dividida por d, deixará a unidade, se tivermos $b = e^4$, ou em geral $b = e^4 \pm \lambda d$. Assim, números menores são resíduos, que surgem da divisão de biquadráticos por d, isto é, devem ser tomados apenas os biquadráticos que são primos com d.

225. Em geral, portanto, se o número μ for divisível por ν, a potência $b^{\frac{\mu}{\nu}}$, dividida por d, deixará a unidade se tomarmos $b = e^\nu$, ou até $e^\nu \pm \lambda d$, de forma que, números apropriados, a serem substituídos por b, são resíduos, que surgem da divisão por d de potências de ordem ν, sendo essas potências primas com d.

226. Basta, portanto, tomar por b os números menores que d, que são primos com ele. Sendo a unidade tomada por b, todos os resíduos serão iguais à unidade, de modo que nesse caso sempre temos $n = 1$, ou seja, $n = \frac{\mu}{\mu}$. Só resta um caso como este, quando tomarmos o divisor $d = 2$, pois isto, decerto, faz com que $\mu = 1$.

227. Seja o divisor $d = 3$. Então, teremos $\mu = 2$, e além do caso $b = 1$, para o qual $n = 1$, teremos o caso $b = 2$, em que surge a seguinte progressão geométrica com seus resíduos:

Progr. geom. $1, 2, 2^2, 2^3, 2^4,$ *etc*, onde temos $n = 2$,
Resíduos $1, 2, 1, 2, 1,$ *etc*., ou seja, $n = \mu$.

228. Seja o divisor $d = 4$. Então, teremos $\mu = 2$, e além do caso $b = 1$, para o qual $n = 1 = \frac{1}{2}\mu$, teremos o caso $b = 3$.

Progr. geom. $1, 3, 3^2, 3^3, 3^4,$ *etc*, aqui temos $n = 2 = \mu$
Resíduos $1, 3, 1, 3, 1,$ *etc*.

229. Seja o divisor $d = 5$. Então, $\mu = 4$ e teremos os seguintes casos

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Progr. geom.	1, 1,	$1,2,2^2,2^3,2^4$	$1,3,3^2,3^3,3^4$	$1, 4, 4^2$
Resíduos	1, 1,	1 2,4, 3, 1	1, 3,4, 2, 1	1, 4, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

em dois desses casos, portanto, temos $n = 4$, num $n = 2$ e num $n = 1$.

230. Seja o divisor $d = 6$. Então, $\mu = 2$ e teremos dois casos

	$b = 1$	$b = 5$
Progr. geom.	1, 1,	$1, 5, 5^2$
Resíduos	1, 1,	1, 5, 1
	$n = 1$	$n = 2$

231. Seja o divisor $d = 7$. Então, $\mu = 6$ e teremos o mesmo número de casos

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Progr. geom.	1,1,	$1, 2,2^2,2^3$	$1, 3, 3^2,3^3,3^4, 3^5\ 3^6$	$1,4,4^2,4^3$
Resíduos	1,1,	1, 2, 4, 1	1 ,3, 2, 6, 4, 5, 1	1, 4, 2, 1
	$n = 1$	$n = 3$	$n = 6$	$n = 3$

	$b = 5$	$b = 6$
Progr. geom.	$1, 5, 5^2, 5^3, 5^4, 5^5, 5^6$	$1, 6, 6^2$
Resíduos	1, 5, 4, 6, 2, 3 1,	1, 6, 1
	$n = 6$	$n = 2$

232. Seja o divisor $d = 8$. Então, teremos $\mu = 4$ e o mesmo número de casos

	$b = 1$	$b = 3$	$b = 5$	$b = 7$
Progr. geom.	1,1,	1, 3, 3^2	1, 5, 5^2	1, 7, 7^2
Resíduos	1,1,	1, 3, 1	1, 5, 1	1, 7, 1
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

não temos, portanto, caso algum em que $n = \mu$, mas em três casos $n = \frac{1}{2}\mu$ e num $n = \frac{1}{4}\mu$.

233. Seja o divisor $d = 9$. Então, $\mu = 6$ e teremos o mesmo número de casos

	$b = 1$	$b = 2$	$b = 4$
Progr. geom.	1,1,	1, 2, 2^2, 2^3, 2^4, 2^5, 2^6	1, 4,4^2, 4^3
Resíduos	1,1,	1, 2, 4, 8, 7, 5, 1	1, 4, 7, 1
	$n = 1$	$n = 6$	$n = 3$

	$b = 5$	$b = 7$	$b = 8$
Progr. geom.	1,5, 5^2, 5^3, 5^4, 5^5, 5^6	1,7, 7^2, 7^3,	1,8, 8^2
Resíduos	1,5, 7, 8, 4, 2, 1	1, 7, 4, 1	1, 8, 1
	$n = 6$	$n = 3$	$n = 2$

234. Seja o divisor $d = 10$. Então, $\mu = 4$

	$b = 1$	$b = 3$	$b = 7$	$b = 9$
Progr. geom.	1, 1,	1, 3, 3^2, 3^3,3^4	1,7,7^2,7^3,7^4	1,9, 9^2
Resíduos	1, 1,	1, 3, 9, 7, 1	1, 7, 9, 3,1	1, 9, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

235. Seja o divisor $d = 11$. Então, $\mu = 10$ e teremos o mesmo número de casos

	$b = 1$	$b = 2$	$b = 3$
Progr. geom.	$1,1,$	$1,2,2^2,2^3,2^4,2^5,2^6,2^7,2^8,2^9,2^{10}$	$1,3,3^2,3^3,3^4,3^5$
Resíduos	$1,1,$	$1,2,4,\ 8,\ 5,\ 10,9,\ 7,\ 3,\ 6,\ 1$	$1,3,9,\ 5,\ 4,\ 1$
	$n = 1$	$n = 10$	$n = 5$

	$b = 4$	$b = 5$
Progr. geom.	$1,\ 4,\ 4^2,\ 4^3,\ 4^4,\ 4^5$	$1,\ 5,\ 5^2,\ 5^3,\ 5^4,\ 5^5$
Resíduos	$1,\ 4,\ 5,\ \ 9,\ \ 3,\ \ 1$	$1,\ 5,\ 3,\ \ 4,\ \ 9\ \ 1$
	$n = 5$	$n = 5$

	$b = 6$	$b = 7$
Progr. geom.	$1,6,6^2,6^3,6^4,6^5,6^6,6^7,6^8,6^9,6^{10}$	$1,7,7^2,7^3,7^4,7^5,7^6,7^7,7^8,7^9,7^{10}$
Resíduos	$1,6,\ 3,7,\ \ 9,10,\ 5,\ 8,\ 4,\ \ 2,\ \ 1$	$1,7,5\ \ 2\ \ 3,\ 10,\ 4,\ 6,\ 9\ \ 8,\ \ 1$
	$n = 10$	$n = 10$

	$b = 8$
Progr. geom.	$1,\ \ 8,\ \ 8^2,\ \ 8^3,\ \ 8^4,\ \ 8^5,\ \ 8^6,\ \ 8^7,\ \ 8^8,\ \ 8^9,\ \ 8^{10}$
Resíduos	$1,\ \ 8,\ \ 9,\ \ \ 6,\ \ \ 4,\ \ 10,\ \ 3,\ \ \ 2,\ \ \ 5,\ \ \ 7,\ \ \ 1$
	$n = 10$

	$b = 9$	$b = 10$
Progr. geom.	$1,\ \ 9,\ \ 9^2,\ \ 9^3,\ \ 9^4,\ \ 9^5$	$1,\ \ 10,\ \ 10^2$
Resíduos	$1,\ \ 9,\ \ 4,\ \ \ 3,\ \ \ 5,\ \ \ 1$	$1,\ \ 10,\ \ \ 1$
	$n = 5$	$n = 2$

236. Seja o divisor $d = 12$. Então, teremos $\mu = 4$ e o mesmo número de casos

	$b = 1$	$b = 5$	$b = 7$	$b = 11$
Progr. geom.	$1,\ \ 1,$	$1,\ 5,\ 5^2$	$1,\ \ 7,\ \ 7^2$	$1,\ \ 11,\ \ 11^2$
Resíduos	$1,\ \ 1,$	$1,\ 5,\ 1$	$1,\ \ 7,\ \ 1,$	$1,\ \ 11,\ \ \ 1$
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

aqui, portanto, sempre temos $n < \mu$, a saber, em três casos $n = \frac{1}{2}\mu$ e num $n = \frac{1}{4}\mu$.

237. Seja o divisor $d = 13$. Então, teremos $\mu = 12$, e, para a menor potência b^n que, dividida por 13, deixa a unidade, acharemos que

se $b =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,
$n =$	1,	12,	3,	6,	4,	12,	12,	4,	3,	6,	12,	2.

238. Do mesmo modo em que, sempre que seja $b = 1$, temos $n = 1$ qualquer que seja o divisor d, assim também, tomando $b = d-1$, temos $n = 2$, ou seja, $(d-1)^2$, dividido por d, deixa a unidade, o que nunca acontece para a primeira potência. Sobre os outros valores assumidos por b, porém, é difícil julgar.

239. Visto que a potência $(kd+1)^n$, dividida por d, deixa 1, se tivermos $kd+1 = bc$ e a potência b^n, dividido por d, também deixar a unidade, então ainda a potência c^n deixará a unidade. Pois, como b^n deixa 1, o produto $b^n c^n$ deixará c^n, mas, por hipótese, $b^n c^n$ deixa 1; logo, c^n será equivalente à unidade no valor do seu resíduo, ou seja, c^n, dividido por d, deixará a unidade.

240. Para essa razão[15], se b^n for a menor potência deixando a unidade quando dividida por d, e sendo $bc = kd+1$, então a menor potência de c deixando a unidade será ou c^n, ou até uma menor, sendo seu expoente uma parte alíquota de n. Contudo, se uma potência menor desse c deixar a unidade, digamos $c^{\frac{n}{\nu}}$, então a mesma potência de b deixará a unidade, que, porém, é contra a hipótese; segue que, se b^n for a menor

[15] N. do Trad. Observe que, em §239, $(kd+1)^n \equiv 1 \pmod{d}$ para *todo n* (natural).

potência deixando a unidade, também c^n será a menor potência deixando 1.

241. Assim, pondo $d = 13$, visto que 5^4 é a menor potência deixando a unidade, se tivermos $5c = 13k+1$, c^4 também será a menor potência deixando a unidade. Na verdade, para fazer $13k+1$ divisível por 5, devemos fazer $k = 5\lambda-2$, e teremos $c = 13\lambda-5$, cujo valor mínimo é $c = 8$, e teremos[16] que 8^4 é a menor potência deixando a unidade quando dividido por 13.

242. Ora, qualquer que seja o número b, menor que d e primo com ele, sempre há um número c, também menor que d e primo com ele, tal que $bc = kd+1$, e não mais. Pois se houvesse dois, tais que tanto $bc = kd+1$, quanto $be = ld+1$, teríamos $bc-be = b(c-e)$ é divisível por d e, em consequência, porque b e d são primos entre si, $c-e$ seria divisível por d; no entanto, como c e e são menores que d, isto não é possível, a não ser que tivermos $e = c$. Pode acontecer, porém, que $c = b$, que sempre ocorre se tivermos ou $b = 1$ ou $b = d-1$.

[16] N. do Trad. Ver §237.

Capítulo VIII

Sobre potências de números que, quando divididos por números primos, deixam a unidade

243. Qualquer que seja o resíduo deixado pela potência a^n, quando dividida por d, o mesmo será deixado por todas as potências $(a+\lambda d)^n$ com o mesmo expoente; de fato, se n for um número par, a potência $(\lambda d-a)^n$ também deixará o mesmo resíduo, o que nos leva a retomar a investigação dos resíduos dos números a, menores que o divisor d.

244. Seja, então, o divisor d um número primo qualquer e, visto que não há dificuldade alguma para dois, ponhamos $d = 2p+1$ e, assim, $2p$ será a quantidade de números menores que d e primos com ele. Se a for um número qualquer primo com d, o que faz com que a não é um múltiplo de d, vimos[1] que a potência a^{2p}, dividido por $d = 2p+1$, sempre deixará a unidade.

245. Frequentemente acontece, porém, que uma potência menor a^n, sendo $n < 2p$, deixa a unidade quando divido por $d = 2p+1$; nesse caso, o expoente n é certamente uma parte alíquota[2] de $2p$. Quando isto acontece, portanto, não somente a fórmula $a^{2p}-1$, mas também a fórmula a^n-1, será divisível pelo número primo $2p+1$.

[1] N. do Trad. Em §213.
[2] N. do Trad. Ver §211.

246. Mas, se a fórmula a^n-1 for divisível pelo número primo $2p+1$, também a fórmula $a^{mn}-1$ será divisível; em consequência, visto que a fórmula $a^{2p}-1$ é seguramente divisível por $2p+1$, a diferença $a^{mn}-a^{2p}$, ou seja $a^{2p}(a^{mn-2p}-1)$, também será divisível. Mas, visto que o fator a^{2p} não admite a referida divisão, o outro fator, $a^{mn-2p}-1$, será necessariamente divisível, qualquer que seja o número tomado para m.

247. Seja λ o máximo divisor comum dos números n e $2p$. Se a fórmula a^n-1 for divisível pelo número primo $2p+1$, então a fórmula $a^{\lambda}-1$ também será divisível por $2p+1$. Pois, sejam $n = \alpha\lambda$ e $2p = \beta\lambda$, onde α e β são números primos entre si, e, visto que tanto $a^{\alpha\lambda}-1$ quanto $a^{\beta\lambda}-1$ são múltiplos de $2p+1$, as fórmulas $a^{\mu\alpha\lambda}-1$ e $a^{\nu\beta\lambda}-1$ também serão múltiplos. Mas, visto que α e β são números primos entre si, μ e ν podem ser encontrados[3] tais que $\mu\alpha = \nu\beta+1$; sua diferença será $a^{\nu\beta\lambda+\lambda}-a^{\nu\beta\lambda} = a^{\nu\beta\lambda}(a^{\lambda}-1)$ e, visto que a mesma é divisível por $2p+1$, é necessário que $a^{\lambda}-1$ seja divisível por $2p+1$.

248. Se, portanto[4], n seja um número primo com $2p$, a forma a^n-1 não pode ser divisível pelo número primo $2p+1$, exceto no caso que $a-1$ seja divisível por ele. Desta forma, se $a-1$

[3] N. do Trad. Isto é observado na margem do Capítulo IV. É fácil encontrar uma combinação linear de dois números igual ao seu MDC através do Algoritmo de Euclides.

[4] N. do Trad. Visto que n e $2p$ são primos entre se, o valor de λ, em §247, será 1.

não for um múltiplo do número primo $2p+1$, a fórmula a^n-1 não é divisível por esse primo, a não ser que n e $2p$ sejam números compostos entre si, cujo máximo divisor comum é λ e, nesse caso, a fórmula $a^\lambda-1$ será divisível por $2p+1$.

249. Assim, se a^n for a menor potência de a, que, dividida pelo número primo $2p+1$, deixa a unidade, então certamente n será uma parte alíquota do número $2p$. Logo, se tivermos $ab = k(2p+1)+1$, então[5] b^n será o menor potência de b, que, dividida por $2p+1$, deixa a unidade.

250. Seja n um número primo tal que a fórmula a^n-1 é divisível pelo número primo $2p+1$, então ou n será uma parte alíquota de $2p$ (pois não há aqui outro divisor comum), ou, se for primo com $2p$, o número $a-1$ será divisível por $2p+1$. Logo, a fórmula a^n-1 não admite outros divisores primos, além dos divisores do próprio $a-1$, exceto os da forma $2p+1$, onde $2p$ é um múltiplo de n. Desta maneira, todos seus divisores primos são contidos na forma $2mn+1$.

251. Por essa razão, a^3-1 não admite, além dos divisores de $a-1$, outros divisores primos, exceto os da forma $6m+1$, que são 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, *etc*. Como $aa+a+1$ é fator de a^3-1, ele também não é divisível por qualquer outro número primo.

[5] N. do Trad. Ver §240.

252. De modo semelhante, a forma a^5-1 não tem outros divisores, além dos divisores de $a-1$, exceto os contidos na forma $10m+1$, os quais são 11, 31, 41, 61, 71, *etc*. Para essa razão, os números

$$a^4+a^3+a^2+a+1,$$

se não sejam primos, não admitem outros divisores.

253. Se quisermos achar números perfeitos, o quociente 2^n-1 deve ser um número primo[6]; mas é evidente que isto não pode acontecer, a não ser que n seja primo. Mas, se n for assim, a fórmula 2^n-1 certamente não pode ter outros divisores exceto os da forma $2mn+1$; donde, a investigação sobre se é primo ou não será mais facilmente resolvida.

254. Como $a^{2p}-1$ sempre é divisível pelo número primo $2p+1$ e sendo essa forma composta dos fatores a^p-1 e a^p+1, um ou outro será necessariamente divisível por $2p+1$. Vimos[7], porém, que, se $a = ee\pm\lambda(2p+1)$, então a^p-1 será divisível; assim, nesse caso, a fórmula a^p+1 certamente não será divisível por $2p+1$.

255. Assim a seguinte questão surge: talvez a fórmula a^p-1 sempre será divisível por $2p+1$? e, portanto, a outra, a^p+1, nunca. No caso em que p é um número ímpar, contudo, é claro

[6] N. do Trad. Ver §107.
[7] N. do Trad. Em §222.

que a resposta é negativa. Pois, visto que, no presente caso, a^p+1 tem o fator $a+1$, é claro que, fazendo $a = 2p$, a referida fórmula será divisível por $2p+1$.

256. Em geral, então, pode ser mostrado, da seguinte maneira, que a fórmula a^n-1, sendo $n < 2p$, nem sempre[8] será divisível pelo número primo $2p+1$; ao contrário, há seguramente números tais que, quando tomados para a, a divisão da fórmula a^n-1 não procede. Isto é demonstrado, de forma bastante cômoda, por absurdo.

257. Pois, quem nega isto tem de afirmar que todas as seguintes fórmulas são divisíveis por $2p+1$: 1^n-1, 2^n-1, 3^n-1, 4^n-1, 5^n-1, ..., n^n-1 e, portanto, também tanto suas primeiras diferenças 2^n-1, 3^n-2^n, 4^n-3^n, 5^n-4^n, *etc*, quanto as segundas $3^n-2\cdot 2^n+1^n$, $4^n-2\cdot 3^n+2^n$, $5^n-2\cdot 4^n+3^n$, *etc*., bem como todas as outras.

258. No entanto, as diferenças da ordem n são constantes, e, indicando-as pela letra N, são expressas da seguinte maneira:

$$N = (n+1)^n - n\cdot n^n + \frac{n(n-1)}{1\cdot 2}(n-1)^n - \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}(n-2)^n + etc.$$

É fácil calcular os valores para essas expressões para vários valores de n:

[8] N. do Trad. Isto é, para todo primo $2p+1$, sempre há algum a tal que a^n-1 não é um múltiplo do referido primo.

Se $n = 1$ temos $N = 2–1 = 1$
$n = 2$ $N = 3^2–2\cdot 2^2+1 = 2 = 1\cdot 2$
$n = 3$ $N = 4^3–3\cdot 3^3+3\cdot 2^3–1 = 6 = 1\cdot 2\cdot 3$
$n = 4$ $N = 5^4–4\cdot 4^4+6\cdot 3^4–4\cdot 2^4+1 = 24 = 1\cdot 2\cdot 3\cdot 4$
etc.

259. Para mostrar isto mais claramente, escrevemos n+1 para n,

$$P = (n+2)^{n+1}–(n+1)(n+1)^{n+1}+\frac{(n+1)n}{1\cdot 2}n^{n+1}–\frac{(n+1)n(n-1)}{1\cdot 2\cdot 3}(n–1)^{n+1}+ etc.$$

e, começando com o termo anterior,

$$P = (n+1)^{n+1}–(n+1)n^{n+1}+\frac{(n+1)n}{1\cdot 2}(n–1)^{n+1}– etc.$$

Mas, o valor de N pode ser representado como

$$N = (n+1)^{n}–n^{n+1}+\frac{n}{1\cdot 2}(n–1)^{n+1}–\frac{n(n-1)}{1\cdot 2\cdot 3}(n–2)^{n+1}+ etc.$$

o que fornecerá o valor de P quando multiplicado por n+1 e, portanto, $P = (n+1)N$.

260. Desta forma, visto que no caso $n = 1$ temos $N = 1$, no caso $n = 2$ teremos $N = 1\cdot 2$, no caso $n = 3$ teremos $N = 1\cdot 2\cdot 3$ e, em geral, para um número n qualquer, teremos $N = 1\cdot 2\cdot 3\cdot ...\cdot n$. Mas, de fato, a diferença de ordem n não é divisível pelo número primo $2p$+1, porque $n < 2p$, do qual segue que nem todos os termos da sequência exibida em §257 são divisíveis pelo referido primo.

261. Seja $6p$+1 um número primo. Embora a forma $a^{6p}–1$ é por ele divisível, a não ser que a seja um múltiplo dele, haverá

também casos em que $a^{2p}-1$ pode ser por ele dividido, por exemplo, fazendo $a = e^3 \pm \lambda(6p+1)$. Não obstante, também haverá casos em que a fórmula $a^{2p}-1$ não será divisível pelo referido primo $6p+1$, como será claro da demonstração feita.

262. Visto que já foi mostrado que $a^{3p}-1$ será divisível por $6p+1$ se tivermos

$$a = cc \pm \lambda(6p+1),$$

podemos deduzir agora que, se o número a for contido em ambas as formas $cc \pm \lambda(6p+1)$ e $c^3 \pm \lambda(6p+1)$, então a fórmula a^p-1 será divisível por $6p+1$, pois teríamos $a = c^6 \pm \lambda(6p+1)$.

263. Se $4p+1$ for um número primo, o que faz $a^{4p}-1$ por ele divisível, então a^p-1 poderá ser dividido por ele, se tivermos $a = c^4 \pm \lambda(4p+1)$. Não obstante, há também casos em que a fórmula a^p-1 não admite essa divisão: os, com certeza, em que ou a^p+1 ou $a^{2p}+1$ são divisíveis por $4p+1$.

Capítulo IX

Sobre divisores de números da forma $a^n \pm b^n$

264. Dado que $2p+1$ é um número primo e que a e b não são múltiplos do mesmo, a fórmula $a^{2p}-1$, bem como $b^{2p}-1$, são divisíveis por esse primo; portanto, também a sua diferença $a^{2p}-b^{2p}$ sempre admite divisão pelo número primo $2p+1$.

265. Consideremos agora o número a^n-b^n, divisível pelo número primo $2p+1$ e, para investigar em que modo isto pode acontecer, seja φ o máximo divisor comum dos números n e $2p$, de tal forma que, fazendo $n = \alpha\varphi$ e $2p = \beta\varphi$, os números α e β serão primos entre si.

266. Ainda mais, como α e β são números primos entre si, podemos fazer com que $\mu\alpha = \nu\beta+1$. Por isto, visto que $a^{\alpha\varphi}-b^{\alpha\varphi}$ e, portanto $a^{\mu\alpha\varphi}-b^{\mu\alpha\varphi}$, é divisível por $2p+1$, teremos que $a^{(\nu\beta+1)\varphi}-b^{(\nu\beta+1)\varphi}$ será divisível, e, porque $a^{\beta\varphi}-b^{\beta\varphi}$ é divisível, também será todo número $a^{\nu\beta\varphi}-b^{\nu\beta\varphi}$, e até o mesmo multiplicado por a^{φ}, a saber, $a^{(\nu\beta+1)\varphi}-a^{\varphi}b^{\nu\beta\varphi}$.

267. Tirando a última forma da precedente, a diferença $a^{\varphi}b^{\nu\beta\varphi}-b^{(\nu\beta+1)\varphi} = b^{\nu\beta\varphi}(a^{\varphi}-b^{\varphi})$ será divisível pelo número primo $2p+1$. Mas, $b^{\nu\beta\varphi}$ não é por ele divisível, portanto o outro fator $a^{\varphi}-b^{\varphi}$ é necessariamente divisível.

268. Assim, se o número $a^n–b^n$ for divisível pelo número primo $2p+1$ e se φ for o máximo divisor comum dos números n e $2p$, então o número $a^\varphi–b^\varphi$ será divisível por $2p+1$ e, se este não admitir a divisão, aquele também não a admitirá.

269. Ora, sendo n e $2p$ primos entre si, ou seja, sendo a unidade seu máximo divisor comum, se $a–b$ não seja divisível por $2p+1$, também $a^n–b^n$ não admitirá a divisão por esse número primo.

270. Ao procurar, portanto, os divisores primos do número $a^n–b^n$, além dos divisores, que se apresentam prontamente, do próprio $a–b$, devemos procurar os restantes entre os números primos $2p+1$, para os quais $2p$ e n não são primos, mas compostos.

271. Assim, se n for um número primo, só devemos olhar para todos os divisores do número $a^n–b^n$, além dos contidos em $a–b$, entre os números primos da forma $\lambda n+1$, se de fato a e b são primos entre si, qual condição, é claro, deve ser acrescentada.

272. Para os vários valores de n, portanto, os divisores primos da forma $a^n–b^n$, além de $a–b$, devem ser procurados, como segue: (*)

da forma	divisores devem ser procurados entre os seguintes números primos:
a^2-b^2	$2\lambda+1$ . . . 3, 5, 7, 11, 13, 17, 19, nenhum[1] é excluído
a^3-b^3	$3\lambda+1$ . . . 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, *etc*.
a^5-b^5	$5\lambda+1$ . . . 11, 31, 41, 61, 71, 101, *etc*.
a^7-b^7	$7\lambda+1$ . . . 29, 43, 71, 113, 127, *etc*.
$a^{11}-b^{11}$	$11\lambda+1$ . . 23, 67, 89, 199, 331, *etc*.
	etc.

(*) *Escrito na margem*: 1. Entre os divisores da forma a^n-b^n, também pode acontecer o próprio número n. 2. De a^3-b^3, segue[2] que o número $aa+ab+bb$ não pode ter outros divisores exceto $3\lambda+1$; logo, $3\lambda-1$ certamente não são divisores.

273. Se n não for um número primo, mas o produto de dois primos, digamos $n = \alpha\beta$, os divisores primos para a forma $a^{\alpha\beta}-b^{\alpha\beta}$, além de $a-b$, serão contidos na forma $2p+1$, sendo $2p$ não primo com $\alpha\beta$ e, em consequência, conforme ou α, ou β, ou $\alpha\beta$ seja o máximo divisor comum, a forma dos divisores primos será ou $\lambda\alpha+1$, ou $\lambda\beta+1$, ou $\lambda\alpha\beta+1$, na primeira dos quais, λ não deve conter β, no segundo, não α e, no terceiro, não há condição.

[1] N. do Trad. Isto é, nenhum número primo ímpar é excluído.
[2] N. do Trad. Os divisores primos de a^3-b^3 são os divisores primos de $a-b$ e os primos contidos na forma $3\lambda+1$. Mas, $a^2+ab+b^2 = (a^3-b^3)/(a-b)$ e o próprio a^2+ab+b^2 não é divisível por a–b. Logo, os divisores de a^2+ab+b^2 devem ser achados entre primos da forma $3\lambda+1$. Esse tipo de raciocínio acontece com frequência nos próximos parágrafos.

274. Mas, divisores da forma $\lambda\alpha+1$ também dividirão $a^{\alpha}-b^{\alpha}$ e divisores da forma $\lambda\beta+1$ também dividirão $a^{\beta}-b^{\beta}$, se, de fato, no primeiro, λ seja primo com β e, no segundo, com α.

275. Assim, se quisermos apenas os divisores da fórmula $a^{\alpha\beta}-b^{\alpha\beta}$, que não dividam ao mesmo tempo nem $a^{\alpha}-b^{\alpha}$, nem $a^{\beta}-b^{\beta}$, devemos procurá-los entre os primos da forma $\lambda\alpha\beta+1$; mas se só queremos excluir divisores da forma $a^{\alpha}-b^{\alpha}$, devemos procurar os restantes entre os números primos $\lambda\beta+1$.

276. Sejam $\alpha = 2$ e $\beta = 2$. Então todos os divisores primos do número a^4-b^4, que não são também divisores de a^2-b^2, serão contidos na forma $4\lambda+1$; portanto, os mesmos serão divisores do número a^2+b^2, donde é claro que números da forma a^2+b^2 não admitem divisores primos diferentes dos que têm a forma $4\lambda+1$.

277. Sejam $\alpha = 3$ e $\beta = 2$. Então, todos os divisores primos do número a^6-b^6, que não são também divisores de a^3-b^3, serão contidos na forma $2\lambda+1$; se, queremos os que também não dividem a^2-b^2, serão achados em $6\lambda+1$. Esses, portanto, serão os divisores[3] da forma a^2-ab+b^2, e tais números não admitem outros divisores.

[3] N. do Trad. Observe que $a^6-b^6 = (a^3-b^3)(a+b)(a^2-ab+b^2)$. Para eliminar os divisores de a^3-b^3 e os de a^2-b^2, é necessário dividir a^6-b^6 pelo MMC de a^3-b^3 e a^2-b^2.

278. Disto, deduzimos que, em geral, para determinar os divisores do número $a^{2m}-b^{2m}$, que não são ao mesmo tempo divisores do número a^m-b^m, isto é, se queremos os divisores do número a^m+b^m, devemos procurá-los entre números primos da forma $2\lambda m+1$. Contudo, podemos ainda excluir o divisor $a+b$, se m seja um número ímpar.

279. Assim, fazemos a seguinte tabela para vários valores de m:

Forma dos números	divisores devem ser procurados entre primos da forma
a^2+b^2	$4\lambda+1$ que são 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97
a^3+b^3	$6\lambda+1$ 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
a^4+b^4	$8\lambda+1$ 17, 41, 73, 89, 97, 113, 137, 193
a^5+b^5	$10\lambda+1$ 11, 31, 41, 61, 71, 101, 131, 151, 181
a^6+b^6	$12\lambda+1$ 13, 37, 61, 73, 97, 109, 157, 181, 193
a^7+b^7	$14\lambda+1$ 29, 43, 71, 113, 127, 197, 211, 239
a^8+b^8	$16\lambda+1$ 17, 97, 113, 193, 241, 257, 337
	etc.

Os casos, em que o expoente é uma potência de dois, devem ser observados antes dos restantes, porque para os restantes os divisores podem ser determinados segundo seus tipos. Os números $a^{2^n}+b^{2^n}$, portanto, não terão outros divisores primos, a não ser os contidos na forma $2^{n+1}\lambda+1$.

280. Mas, $a^n–b^n$ poderá ser dividido pelo número primo $mn+1$, se os números a e b forem escolhidos de tal forma que $ax^m–by^m$ seja divisível por $mn+1$; sob a condição de que números podem ser determinados para x e y, de tal maneira a satisfazer a referida fórmula, então $a^n–b^n$ certamente será divisível por $mn+1$.

281. Pois[4], se $ax^m–by^m$ for divisível por $mn+1$, então também $a^nx^{mn}–b^ny^{mn}$ será divisível. Mas a forma $x^{mn}–y^{mn}$ sempre é divisível e, portanto, também $a^nx^{mn}–a^ny^{mn}$ e, consequentemente, a diferença $a^ny^{mn}–b^ny^{mn}$ e, logo, também $a^n–b^n$ será divisível pelo número primo $mn+1$

282. Se, portanto, números são tomados para a e b tais que $a^n–b^n$ não seja divisível por qualquer número primo $mn+1$, então não haverá valores para x e y tais que $ax^m–by^m$ admite a divisão pelo número primo $mn+1$, exceto quando cada um dos números x e y seja um múltiplo do mesmo. Seja entendido, então, que x e y sejam primos entre si.

283. Assim, visto que $2^2–1$ é divisível apenas por 3, se $2m+1$ for um número primo, então, exceto por $m = 1$, nenhum número contido na forma $2x^m–y^m$ pode ser dividido pelo número primo $2m+1$:

[4] N. do Trad. Observe: para a primeira inferência, $a^nx^{mn}–b^ny^{mn} = (ax^m)^n–(by^m)^n$; para a segunda e quarta, §214 com x e y supostos primos com o número primo $mn+1$; e para a terceira, a diferença é $(a^nx^{mn}–b^ny^{mn})–(a^nx^{mn}–a^ny^{mn})$.

assim dado	nenhum número	será divisível por
$m = 2$	$2x^2 - y^2$	5
$m = 3$	$2x^3 - y^3$	7
$m = 5$	$2x^5 - y^5$	11
$m = 6$	$2x^6 - y^6$	13
	etc.	

Capítulo X

Sobre resíduos surgidos da divisão de quadrados por números primos

284. O resíduo que é deixado, quando um quadrado a^2 é dividido por um número d qualquer, é o mesmo que é deixado quando qualquer dos infinitos quadrados $(nd \pm a)^2$ é dividido pelo número d.

285. Para essa razão, se quisermos examinar os resíduos que são deixados pela divisão de números quadrados por um dado número d, bastará considerar quadrados, cujas raízes são menores que o divisor d, a saber,

$$1, 4, 9, 16, ..., (d-4)^2, (d-3)^2, (d-2)^2, (d-1)^2,$$

cuja quantidade é $d-1$.

286. Mas, os quadrados extremos 1 e $(d-1)^2$, bem como quaisquer dois igualmente removidos dos extremos, dão os mesmos resíduos; em consequência, se $d-1$ é um número par, não poderá haver mais resíduos distintos que $\frac{1}{2}(d-1)$, e se $d-1$ é um número ímpar, devido ao termo único no meio, que $\frac{1}{2}d$.

287. Agora seja d um número primo e, porque o caso de dois é claro, ponhamos $d = 2p+1$. Ora, todos os resíduos resultarão dos quadrados 1, 4, 9, ..., $(p-2)^2$, $(p-1)^2$, p^2, cuja

quantidade não pode ser maior que p; disto, é claro que nem todos os números menores que $d = 2p+1$, cuja quantidade é $2p$, ocorrem entre os resíduos, mas, no mínimo, metade deles são excluídos.

288. Em primeiro lugar, então, digo que todos os resíduos oriundos desses quadrados, 1, 4, 9, ..., p^2, são distintos; pois, se dois quadrados, não maiores que p^2, digamos m^2 e n^2, dessem o mesmo resíduo, sua diferença m^2-n^2 e, portanto, ou $m-n$, ou $m+n$, seria divisível pelo número primo $d = 2p+1$, o que não é possível, visto que, para $m < \frac{1}{2}d$ e $n < \frac{1}{2}d$, $m+n$ é menor que d.

289. Visto, portanto, que todos os resíduos, que surgem da divisão dos quadrados 1, 4, 9, ..., p^2 pelo número primo $d = 2p+1$, são distintos, vamos representá-los assim:

raízes	1	2	3	4	5	6	...	p
quadrados	1	4	9	16	25	36	...	p^2
resíduos	1	α	β	γ	δ	ε	...	π

e a quantidade desses resíduos será $= p$.

290. Como a quantidade de todos os números menores que o divisor $2p+1$, que, ao mesmo tempo, são primos com ele, é $= 2p$, será claro que metade desses números é excluída da classe dos resíduos e, portanto, chamá-los-emos *não-resíduos*. Assim, a quantidade de não-resíduos será exatamente $= p$ e indicaremos os mesmos por letras germânicas $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc*.

291. Se, portanto, acharmos, para qualquer divisor primo $2p+1$, os referidos não-resíduos, poderemos afirmar que não há quadrado algum xx, tal que $xx-\mathfrak{A}$ seja divisível por $2p+1$, onde $\mathfrak{A}$ denota um não-resíduo qualquer. E, de fato, para $2p+1$, tantas fórmulas diferentes desse tipo, $xx-\mathfrak{A}$, podem ser exibidas, quanto p contém de unidades.

292. Assim, para qualquer divisor primo $2p+1$, os números, que são menores que o mesmo, separam-se em duas classes, das quais uma compreende os resíduos e outra os não-resíduos, sendo que cada uma contém a mesma quantidade de números, de tal forma que, por assim dizer, cada não-resíduo corresponde a um resíduo. Desta maneira, convém investigar mais cuidadosamente a natureza dessas duas classes.

293. Se houver dois números m e n na classe dos resíduos, seu produto mn, ou um resíduo equivalente ao mesmo, estará na mesma classe. Pois, se o resíduo m, por exemplo, surgir do quadrado a^2 e n do quadrado b^2, o resíduo mn surgirá do produto a^2b^2, que é também um quadrado.

294. Assim, se um número qualquer m estiver entre os resíduos, todas as suas potências m^2, m^3, m^4, *etc*. serão achadas entre os mesmos, ou melhor, serão equivalentes a resíduos. Se, ainda mais, o número n estiver presente entre os resíduos, então

os números mn, m^2n, mn^2 e, em geral, $m^\mu n^\nu$ também estarão presentes nessa mesma classe.

295. A classe dos resíduos 1, α, β, ... π, para qualquer divisor primo $2p+1$, tem, portanto, a notável propriedade de que o produto de dois ou mais dos seus termos, quaisquer que sejam, pertencem à própria classe, se, de acordo com a natureza de resíduos, reduzimo-los aos seus valores mínimos.

296. Isto merece bastante atenção, pois o número de termos de uma classe de resíduos é determinado, sendo a sua quantidade = p, o mesmo número de não-resíduos sendo excluídos. Mas, não obstante a maneira em que os resíduos se combinarem por multiplicação, sempre o mesmo número deles será contido na referida classe.

297. Seja m um número qualquer ocorrendo na classe de resíduos, sendo $2p+1$ o divisor primo. Vimos[1] acima que, se os termos da progressão geométrica 1, m, m^2, m^3, m^4, *etc*. forem divididos por $2p+1$, todos os produtos de dois deles serão contidos entre os resíduos. E, assim, nenhum número ocorrerá nos resíduos dessas potências, que não é achado também nos resíduos dos quadrados.[2]

[1] N. do Trad. Ver §204.
[2] N. do Trad. Observe que isto não pode ser generalizado, pois, embora m^k será um resíduo quadrático se m for um resíduo quadrático, se n não for um resíduo quadrático, n^k poderá ser um resíduo.

298. Visto que a quantidade de resíduos oriundos das potências não pode superar a quantidade surgida dos quadrados[3], a qual é = p, é claro que ou a potência m^p, ou talvez uma inferior, fornecerá um resíduo = 1. Isto já foi esclarecido[4], pois se m surgir do quadrado aa, teremos $m = aa–k(2p+1)$ e $m^p–1$ é claramente divisível pelo número primo $2p+1$.

299. Mas, voltando aos resíduos de quadrados, vamos observar que, se os números m e mn ocorrem entre os mesmos, então é necessário que o número n também seja achado entre eles. Pois, se o resíduo m surgir do quadrado aa e mn do quadrado bb, então o resíduo mn surgirá de naa e, em consequência, $bb–naa$ será divisível por $2p+1$, sendo a e b primos com $2p+1$.

300. Mas, se $bb–naa$ for divisível por $2p+1$, também $(b+k(2p+1))^2–naa$ será divisível. É sempre permitido[5], porém, tomar k tal que $b+k(2p+1) = ac$, ou seja, tal que $k(2p+1)$, dividido por a, deixa b. Há, portanto, um número c, tal que $aacc–naa$, ou seja, $cc–n$, é divisível por $2p+1$ e, em consequência, o quadrado cc dará resíduo n.

301. Se o número α estiver na classe dos resíduos e o número $\mathfrak{A}$ na dos não-resíduos, o produto $\alpha\mathfrak{A}$ seguramente será

[3] N. do Trad. De novo, isto é para potências de um resíduo quadrático.
[4] N. do Trad. Ver §222.
[5] N. do Trad. Ver a nota de Euler (*), após §139.

achado na classe dos não-resíduos. Pois, se estivesse na classe dos resíduos, $\mathfrak{A}$ também seria na mesma classe, contra a hipótese.

302. Se o produto *mn* ocorrer na classe dos resíduos e um dos seus fatores, *m*, na classe dos não-resíduos, o outro, *n*, certamente será achado na mesma classe dos não-resíduos; pois, se *n* estivesse na classe dos resíduos, também *m* pertenceria à mesma classe.

303. Sejam $\mathfrak{A}$ e $\mathfrak{B}$ dois não-resíduos. Então seu produto cairá na classe dos resíduos. Pois, como todo quadrado ocorre na classe dos resíduos, é evidente, primeiro, que todo quadrado $\mathfrak{A}^2$, $\mathfrak{B}^2$, $\mathfrak{C}^2$, *etc*. nela ocorre; desta forma, ainda falta mostrar que também o produto dos dois, $\mathfrak{AB}$, será achado na mesma classe, mas isso será estabelecido pela seguinte demonstração.

304. Sendo conhecidos os resíduos 1, α, β, γ, *etc*., cuja quantidade é = *p*, e sendo 2*p*+1 o divisor primo, a quantidade dos não-resíduos em relação ao mesmo divisor, visto que são o restante dos números menores que 2*p*+1, é do mesmo modo = *p*. Mas, dado um não-resíduo $\mathfrak{A}$, todos os outros são determinados a partir dos resíduos da seguinte maneira: $\mathfrak{A}$, $\alpha\mathfrak{A}$, $\beta\mathfrak{A}$, $\gamma\mathfrak{A}$, *etc*. feita, é certo, a redução aos menores termos. Pois, esses números são todos distintos e sua quantidade é = *p*.

305. Portanto, dois não-resíduos quaisquer $\mathfrak{D}$ e $\mathfrak{E}$ podem ser considerados desta maneira como os produtos $\delta\mathfrak{A}$ e $\varepsilon\mathfrak{A}$, onde δ e ε são resíduos e $\mathfrak{A}$ um não-resíduo; em consequência, o produto de quaisquer dois não-resíduos será $\mathfrak{DE} = \delta\varepsilon\mathfrak{AA}$, onde $\delta\varepsilon$, visto que é o produto de dois resíduos, é achado na classe dos resíduos.

306. E, de fato, $\mathfrak{AA}$ também ocorre na classe dos resíduos, porque todos os quadrados, ou os resíduos equivalentes, são achados nessa classe. Por isso, como tanto $\delta\varepsilon$ quanto $\mathfrak{AA}$ são resíduos, seu produto $\mathfrak{DE}$ é necessariamente um resíduo e, desta forma, o produto de dois não-resíduos quaisquer é certamente contido na classe de resíduos.

307. Juntando dois números de acordo com sua natureza de ser resíduos ou não-resíduos, portanto, teremos os seguintes resultados:

1. O produto de dois resíduos é um resíduo.
2. O produto de um resíduo e um não-resíduo é um não-resíduo.
3. O produto de dois não-resíduos é um resíduo.

308. Essas coisas serão amplamente ilustradas se observamos alguns resíduos e não-resíduos da divisão de quadrados por número primos[6]:

divisor	3	5	7	11
resíduos	1	1, 4	1, 4, 2	1, 4, 9, 5, 3
não-resíduos	2	2, 3	3, 5, 6	2, 6, 7, 8, 10

divisor	13	17
resíduos	1, 4, 9, 3, 12, 10	1, 4, 9, 16, 8, 2, 15, 13
não-resíduos	2, 5, 6, 7, 8, 11	3, 5, 6, 7, 10, 11, 12, 14

divisor	19	23
resíduos	1,4,9,16, 6, 17, 11, 7, 5	1, 4, 9, 16, 2, 13, 3, 18,12, 8, 6
não-resíduos	2,3,8,10,12,13,14,15,18	5, 7,10,11,14,15,17,19,20,21,22

divisor	29
resíduos	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
não-resíduos	2,3, 8,10, 11,12,14, 1 17, 18, 19, 21, 26, 27 (*)

(*) *Escrito na margem*: Divisor: 59. Resíduos: 1, –2, 3, 4, 5, –6, 7, –8, 9, –10, –11, 12, –13, –14, 15, 16, 17, –18, 19, 20, 21, 22, –23, –24, 25, 26, 27, 28, 29. Portanto, se $4n-1$ é primo, ou $xx+myy$, ou $xx-myy$ é divisível por ele[7].

[6] N. do Trad. O texto original tem, para o divisor 23, 11 entre os resíduos e 12 entre os não-resíduos.

[7] N. do Trad. Novamente a proposição não será verdadeira, se entendermos, como parece indicar a própria formulação da mesma, que todas as variáveis são arbitrárias. Se entendermos, no entanto, a proposição como afirmando que "para todo m, y, existe um x tal que $x^2 \pm my^2$ é divisível pelo primo $4n-1$," então a proposição será verdadeira. Ainda mais, a proposição análoga para primos da forma $4n+1$ não é verdadeira. Para

309. Chamamos o número, que, somado ao resíduo, faz o divisor, o *complemento* do resíduo. Assim, sendo o divisor = d e um resíduo qualquer = r, seu complemento será $d-r$.

310. Se o complemento de um resíduo qualquer ocorrer na classe dos resíduos, então os complementos de todos os resíduos também ocorrerão na mesma classe. Pois, se $d-\alpha$ ocorrer na classe dos resíduos, $1, \alpha, \beta, \gamma, \delta$, *etc*., sendo d o divisor, o resíduo $d-\alpha$ pode ser representado por $-\alpha = -1\cdot\alpha$ e, em consequência, visto que tanto α quanto o produto $-1\cdot\alpha$ são resíduos, também -1 será um resíduo[8] e, portanto, também $-\beta$, $-\gamma$, $-\delta$, *etc*.; mas, esses números são equivalentes aos complementos do restante dos resíduos.

311. Desta forma, ou nenhum ou todos os complementos dos resíduos ocorrerão na sequência de resíduos. Será claro, dos exemplos acima[9], que, se o divisor for ou 3, ou 7, ou 11, ou 19, ou 23, nenhum complemento será achado nos resíduos, mas os mesmos serão todos não-resíduos. Mas, se o divisor for 5, ou 13, ou 17, ou 29, os diversos complementos serão achados na classe dos resíduos.

$m = 7$ e $y = 3$, por exemplo, não existe x algum tal que 17 divide $x^2 \pm my^2$, ou seja, $\frac{x^2 \pm 63}{17}$ não é inteiro se x é inteiro.

[8] N. do Trad. Ver §299 ou §307.

[9] N. do Trad. Ver §308.

312. Se o divisor for o número primo $2p+1$ e os complementos dos diversos resíduos ocorrerem nos resíduos, visto que serão relacionados entre si dois a dois de tal maneira que um é o complemento do outro – e nem pode acontecer que qualquer um seja seu próprio complemento, pois $2p+1$ não admite uma metade[10] –, a quantidade de resíduos será necessariamente par.

313. Logo, como a quantidade dos resíduos é $= p$, não é possível que os complementos dos resíduos também sejam resíduos, a não ser que p seja par. Assim, se p for um número ímpar, é certo que nenhum complemento de um resíduo será contido na classe dos resíduos e, portanto, os complementos de todos os resíduos constituirão a classe de não-resíduos.

314. Seja, então, p um número ímpar $= 2q-1$, de tal forma que o divisor primo seja $= 4q-1$ e, assim, os complementos de todos os resíduos serão não-resíduos. Desta maneira, se α for um resíduo qualquer, seu complemento $4q-1-\alpha$ será um não-resíduo, ou seja, não há quadrado algum que, quando dividido por $4q-1$, deixa $4q-1-\alpha$.

[10] N. do Trad. Isto é, seja c é o complemento do resíduo r; se tivéssemos $c = r$, visto que $c = d-r$, teríamos $r = \frac{d}{2}$, o que é impossível quando $d = 2p+1$. Mas, c é algum resíduo, $r' \neq r$. Seja, então, $c_i = r_i'$ o complemento do resíduo r_i. Então, os resíduos serão $r_1, r_1', r_2, r_2', \ldots r_k, r_k'$, onde $p = 2k$.

315. Visto que α pode se referir a um quadrado qualquer, digamos *nn*, não há quadrado algum que faz o número $4q-1-nn$ divisível por $4q-1$. Assim, $mm-(4q-1-nn)$, ou seja, $mm+nn$, nunca será divisível por um número primo da forma $4q-1$, a não ser que, por acaso, cada um dos números *m* e *n* seja por ele divisível.

316. É demonstrado, portanto, que a soma de dois quadrados, primos entre si, não pode ser dividido por qualquer número primo da forma $4q-1$. Assim, sempre que a soma de dois quadrados desse tipo tiver divisores primos, os mesmos certamente terão a forma $4q+1$, descontando, evidentemente, o número 2, que também pode ser um divisor, no caso em que os dois quadrados são tomados como ímpares.

317. Quando os complementos dos resíduos forem encontrados entre os resíduos, os complementos dos não-resíduos[11] também serão não-resíduos; e, de fato, se o complemento de um resíduo for um não-resíduo, os complementos de todos os resíduos serão não-resíduos, mas os complementos de todos os não-resíduos, por sua vez, serão resíduos.

[11] N. do Trad. Observe que em §309 Euler definiu complementos em referência a resíduos e agora implicitamente estende a definição a não-resíduos. Alternativamente, pode-se entender a definição original como sendo em referência, não a resíduos surgidos de quadrados, mas a resíduos surgidos de qualquer número dividido por um número primo (ver §203).

318. Seja o divisor $2p+1$, sendo p um número par. Será somente nesse caso que pode acontecer que os complementos dos resíduos sejam resíduos; que sempre serão resíduos, porém, ainda não foi demonstrado. Para tanto, esses resíduos devem ser comparados com os resíduos surgidos da série das potências, em relação ao mesmo divisor $2p+1$, se a série de potências com que é comparada tenha uma quantidade igual de resíduos e não-resíduos.

319. Seja 1, a, a^2, a^3, *etc*. uma série de potências desse tipo, que fornece p resíduos distintos[12], quando divido pelo número primo = $2p+1$; deste modo, todos os resíduos serão 1, a, a^2, a^3, ..., a^{p-1}, isto é, as próprias potências a serem usadas como os resíduos equivalentes a estas. Há, portanto, a mesma quantidade de não-resíduos, que são expressos da seguinte maneira: A, Aa, Aa^2, Aa^3, ..., Aa^{p-1}.

320. Ora, esses resíduos, exatamente como os resíduos dos quadrados, são constituídos de tal forma que 1) começam com a unidade, 2) o produto de quaisquer dois resíduos será um resíduo, 3) o produto de um resíduo e um não-resíduo ocorrerá entre os não-resíduos, donde podemos concluir que o produto de dois não-resíduos estará na classe dos resíduos.[13]

---

[12] N. do Trad. Ver §219.

[13] N. do Trad. Para (2) e (3), ver, respectivamente, §204 e §207. Para a consequência, sejam A e B não-resíduos; então B é um dos elementos da sequência de não-resíduos dada no parágrafo anterior, digamos Aa^k. Logo, $AB = Aa^k$ e, em consequência $B = a^k$, um resíduo, contra a hipótese.

321. Se a^p-1 é divisível por $2p+1$, então a certamente é o resíduo de um quadrado. Pois, se fosse um não-resíduo, todos os resíduos restantes, que são $a\alpha$, $a\beta$, $a\gamma$, *etc*., teriam a mesma propriedade e, portanto, todos esses números x seriam tais que x^p-1 poderia ser dividido por $2p+1$, o que é absurdo. (*)

(*) *O presente parágrafo foi escrito na margem.*[14]

322. Pois[15], visto que entre os resíduos dos quadrados temos que a quantidade de não-resíduos é igual à quantidade de resíduos, se, ao contrário, acontecesse, nos resíduos das potências, que o produto de dois não-resíduos desse um não-resíduo, a quantidade de não-resíduos superaria a quantidade de resíduos, contra a hipótese.

323. Isto pode ser mostrado rigorosamente da seguinte maneira: Seja A um não-resíduo qualquer; então qualquer outro não-resíduo pode ser representado como Aa^n e o produto de dois não-resíduos será AAa^n, que, se fosse um não-resíduo, seria equivalente a algo da forma Aa^m, ou $Aa^{m+\nu p}$, de tal forma que podemos considerar m maior que n e, assim, a diferença $Aa^m - AAa^n$ seria divisível por $2p+1$.

[14] N. do Trad. Essa nota (*) se deve aos editores do texto latino.
[15] N. do Trad. Como a nota (*), indica, §321 foi escrito na margem. Assim, o presente parágrafo remonta a §320, que afirma que podemos deduzir que o produto de dois não-resíduos é um resíduo. O raciocínio de Euler parece ser que, se AB fosse um não-resíduo, devido ao argumento da nossa nota anterior, teria de ser distinto de cada um dos elementos da sequência de não-resíduos dada em §319.

324. Mas, como nem A nem a^n pode ser dividido por $2p+1$, $a^{m-n}-A$ seria divisível por $2p+1$, ou seja, a potência a^{m-n}, dividida por $2p+1$, deixaria resíduo A. Mas, como A não é um resíduo, segue que a hipótese é absurda e, portanto, o produto de dois não-resíduos não é contido na forma Aa^m, que caracteriza todo não-resíduo, e, portanto, deve necessariamente ocorrer entre os resíduos.

325. Em consequência, se a seja um número tal que a^p é a menor potência que deixa a unidade, quando dividido pelo número primo $2p+1$, e, portanto, surgem, pela divisão dos termos da progressão geométrica $1, a, a^2, a^3, a^4, ..., a^{p-1}$, tantos resíduos distintos quanto p tem de unidades, e há o mesmo tanto de não-resíduos, é certo que todo produto de dois não-resíduos é contido na classe de resíduos.

326. Mas, visto que todo número menor que o divisor $2p+1$ é contido ou nos resíduos, ou nos não-resíduos, seus quadrados ocorrerão, certamente, na classe dos resíduos[16], e visto que também ocorrem nos resíduos surgidos dos quadrados, segue que ambas as classes de resíduos, tanto os que surgem dos quadrados, quanto os que surgem da referida progressão geométrica, claramente são congruentes uma à outra.

[16] N. do Trad. Pois, resíduo × resíduo = resíduo e não-resíduo × não-resíduo = resíduo.

327. Mas se, para um divisor primo $2p+1$, os números 1, α, β, γ, δ, *etc*. são resíduos surgidos de quadrados, e se $\mathfrak{A}$ for um não-resíduo qualquer, o número $\mathfrak{A}$ também será achado entre os não-resíduos, que correspondam à progressão geométrica 1, a, a^2, a^3, ..., a^{p-1}, onde a^p é a menor potência fornecendo a unidade como resíduo.

328. Já vimos[17] acima que, se a for um resíduo surgido dos quadrados, a^p-1 certamente será divisível por $2p+1$; assim, agora será claro que, se a for um não-resíduo com respeito aos quadrados, então a^p não será a menor potência desse a que deixa a unidade quando dividida por $2p+1$. Logo, ou não deixa a unidade, ou há também uma menor, $a^{\frac{p}{\nu}}$, que deixa a unidade.

329. Seja a um número tal que sua potência a^p, dividida pelo número primo $2p+1$, deixa a unidade; então, a certamente será contido entre os resíduos dos quadrados. Isto é evidente se a^p seja a menor potência desse tipo. Mas, se não for a menor, é aparente que, exatamente por isto, será verdadeiro para uma maior. Pois, se fosse menor, certos desses resíduos, cuja quantidade é p, passariam para a classe dos não-resíduos. Se, por exemplo, $a^{\frac{1}{2}p}$ for o menor, então a será entre os resíduos dos

[17] N. do Trad. Ver §298. A recíproca, dado as condições do problema, é enunciada em §321. É uma consequência de §326.

biquadráticos, mas se for $a^{\frac{1}{3}p}$, então será entre os resíduos das sextas potências, *etc*., de tal forma que *a* será sempre contido entre os resíduos dos quadrados.

330. Se, portanto, *a* for um não-resíduo em relação aos quadrados, então a^p-1 certamente não será divisível por $2p+1$; em consequência, se *a* for o complemento de algum resíduo, digamos $a = d-\alpha$, pondo $d = 2p+1$, então $(d-\alpha)^p-1$ não será divisível por $2p+1$, mas α^p-1 certamente é divisível, pois α é resíduo, e, assim, a diferença $(d-\alpha)^p-\alpha^p$ também não será divisível.

331. Não obstante, essa diferença seria divisível se *p* fosse um número par; para essa razão, a não ser que *p* seja um número ímpar, aquela condição, pela qual assumimos que $(d-\alpha)^p-1$ não é divisível por $2p+1$, ou seja, $d-\alpha$ é um não-resíduo[18], não pode subsistir.

332. Mas, se *p* for um número par, o complemento de qualquer resíduo α, digamos $d-\alpha$, certamente será um resíduo, pois $(d-\alpha)^p-1$ é divisível por $2p+1$; se for um não-resíduo, essa divisão não poderá ocorrer.

333. Se tivermos $p = 2q$ e o número primo proposto para o divisor $= 4q+1$, então os complementos dos vários resíduos

[18] N. do Trad. Se *p* é par, $(d-\alpha)^p$ é um quadrado perfeito e, portando, um resíduo.

serão achados entre os resíduos dos quadrados, isto é, se os resíduos forem 1, α, β, γ, *etc*., também serão resíduos -1, $-\alpha$, $-\beta$, $-\gamma$, *etc*.[19]

334. Portanto, para qualquer quadrado tomado da progressão 1, 4, 9, 16, ..., $4qq$, há um outro, que, adicionado ao primeiro, produz uma soma divisível por $4q+1$, ou seja, visto que a quantidade desses quadrados é $= 2q$ e cada um tem seu par, há q pares distintos de quadrados, cujas somas são divisíveis por $4q+1$. (*)

(*) *Escrito na margem*: Sempre pode-se exibir dois quadrados, cujo soma é divisível pelo número primo $4q+1$ e, de fato, um dos quadrados pode ser escolhido arbitrariamente.

335. E, porque cada quadrado não supera $4qq$, a soma de dois deles é certamente menor que $8qq$; em consequência, se a referida soma é dividida por $4q+1$, o quociente certamente será menor que $2q$. Esse quociente, exceto quando $= 2$, será ou um número primo da forma $4n+1$, ou algum produto de tais primos (§316).

336. Sempre que o divisor primo é da forma $4q+1$, além do número[20] q, o número $4q$, o que é equivalente a -1, que é, por assim dizer, a unidade dos complementos, ocorrerá entre os

[19] N. do Trad. Isto responde à pergunta feita em §318.
[20] N. do Trad. Ver §302.

resíduos dos quadrados; desta forma, todos os restantes dos quadrados negativas, –4, –9, –16, *etc*., ocorrerão no mesmo lugar. Em consequência, os resíduos, tomados conjuntamente, compreenderão tanto os próprios quadrados, quanto os mesmos tomados negativamente; ao multiplicar todos por um deles e ao trazê-los às formas mínimas através de divisão por $4q+1$, haverá $2q$ resíduos, sendo o mesmo tanto excluído.

337. Mas se, ao contrário, o divisor primo for da forma $4q-1$, então –1 e todos os quadrados negativos estarão entre os não-resíduos (*). Pois, se –1 fosse um resíduo, $(-1)^{2q-1}-1$ seria divisível[21] por $4q-1$, o que não é possível. Ainda mais, no caso precedente, se –1 fosse um não-resíduo, sendo o divisor $4q+1$, então $(-1)^{2q}-1$ não seria divisível por $4q+1$, o que também é falso.

(*) *Escrito na margem*: Não há, portanto, uma soma de dois quadrados divisível por um número primo $4q-1$.

338. Mas, somente quadrados são sempre achados na classe dos resíduos; os outros números, dependendo do divisor, às vezes caem entre os resíduos e às vezes entre os não-resíduos, da mesma forma em que acabamos de ver que –1 é um resíduo, se o divisor é $4q+1$, e –1 é um não-resíduo, se o divisor é $4q-1$.

339. Para certos números não-quadrados uma distinção semelhante pode ser observada. O número +2, por exemplo, é

[21] N. do Trad. Isto é, para o divisor primo $2p+1 = 4q-1$, $p = 2q-1$.

achado entre os resíduos sempre que o divisor primo tem ou a forma $8q+1$, ou $8q-1$ (ou seja, $8q+7$). Nos outros casos, nos quais o divisor é ou $8q+3$, ou $8q+5$, o número +2 ocupa um lugar entre os não-resíduos. (**)

(**) *Escrito na margem*: Mas isto, diferente do precedente, não pode ser munido de uma demonstração[22].

340. Mas, o número –2 ocorrerá entre os resíduos nos casos, em que o divisor primo for ou $8q+1$, ou $8q+3$; o mesmo número –2 cai entre os não-resíduos nos casos, em que o divisor primo é ou $8q+5$, ou $8q+7$.

341. Novamente, o número +3 será um resíduo, se o divisor primo for ou $12q+1$, ou $12q+11$; será um não-resíduo, se o divisor for ou $12q+5$, ou $12q+7$. O número –3, porém, será um resíduo, se o divisor primo for ou $12q+1$, ou $12q+7$; e será um não-resíduo, se o divisor for $12q+5$, ou $12q+11$.

342. O número +4 sempre pertencerá aos resíduos e sobre –4 a decisão será a mesma como para –1. O número 5 será achado entre os resíduos, se o divisor for ou $20q+1$, ou $20q+9$, ou $20q+11$, ou $20q+19$; e –5 será descoberto entre os resíduos, se o divisor for ou $20q+1$, ou $20q+3$, ou $20q+7$, ou $20q+9$.

[22] N. do Trad. Ver também §459.

343. Colecionamos esses resultados, para que sejam exibidos a um único olhar:

Entre resíduos será o número	se o divisor primo for
+1	$4q+(1,\ 3)$
–1	$4q+1$
+2	$8q+(1,\ 7)$ (*)
–2	$8q+(1,\ 3)$
+3	$12q+(1,\ 11)$
–3	$12q+(1,\ 7)$
+5	$20q+(1,\ 9,\ 11,\ 19)$
–5	$20q+(1,\ 3,\ 7,\ 9)$
+6	$24q+(1,\ 5,\ 19,\ 23)$
–6	$24q+(1,\ 5,\ 7,\ 11)$
+7	$28q+(1,\ 3,\ 9,\ 19,\ 25,\ 27)$
–7	$28q+(1,\ 9,\ 11,\ 15,\ 23,\ 25)$
+10	$40q+(1,\ 3,\ 9,\ 13,\ 27,\ 31,\ 37,\ 39)$
–10	$40q+(1,\ 7,\ 9,\ 11,\ 13,\ 19,\ 23,\ 37)$
+11	$44q+(1,\ 9,\ 25,\ 5,\ 7,\ 37,\ 39,\ 19,\ 35,\ 43)$
–11	$44q+(1,\ 9,\ 25,\ 5,\ 37,\ 3,\ 15,\ 23,\ 27,\ 31)$
+12	$48q+(1,\ 11,\ 13,\ 23,\ 25,\ 35,\ 37,\ 47)$
–12	$48q+(1,\ 13,\ 25,\ 37,\ 7,\ 19,\ 31,\ 43)$
+14	$56q+(1,\ 5,\ 9,\ 13, 25, 45, 11, 31, 43, 47, 51,55)$
–14	$56q+(1,\ 5,\ 9,\ 13, 25, 45, 3, 15, 19, 23, 27, 39)$
+15	$60q+(1,\ 7,\ 11,\ 17,\ 43,\ 49,\ 53,\ 59)$
–15	$60q+(1,\ 17,\ 49,\ 53,\ 19,\ 23,\ 31,\ 47)$ (**)
	etc.

(*) *Escrito na margem*: $xx-2yy$ não admite divisores primos diferentes de $8q+(1, 7)$.

(**) *Escrito na margem*: 1) Se $xx = mn+r$, então xx, dividido tanto por m, quanto por n, deixará o resíduo r. Portanto, se o resíduo comporta o divisor m, também comporta o divisor n.

2) Se

Divisor	entre não-resíduo	resíduo
$4n-1$	-1	$+2$
$8n-1$	-2	
$8n-3$	± 2	$+3$
$12n-1$	-3	
$12n-7$	± 3	
$8n\pm 3$	$+2$	

Isto pode ser demonstrado; mais ainda, se o divisor é $8n+1$, então $+2$ está entre os resíduos, o que, porém, não é demonstrado aqui.

344. Até esse ponto as coisas dependem apenas de indução[23], mas, ao procurar demonstrações, ajudará ter observado as seguintes coisas. Primeiro, um número $\pm n$ qualquer será achado entre os resíduos, se o divisor primo for da forma $4nq+1$, ou até $4nq+ii$, onde i denota um número ímpar

[23] N. do Trad. Isto é, investigação de casos específicos, não Indução Matemática. As "seguintes coisas" são generalizações a partir da informação apresentada nas tabelas do parágrafo anterior, onde i é tomado coprimo com n.

qualquer. Segundo, o número positivo $+n$ será um resíduo, se o divisor primo for da forma $4nq-1$, ou, em geral, $4nq-ii$; para esses divisores, no entanto, o número negativo $-n$ será achado entre os não-resíduos.

345. Se o número positivo n for um resíduo para o divisor d, também será um resíduo para qualquer divisor da forma $4nq \pm d$, ou até $4nq \pm dii$; e se o número negativo $-n$ for um resíduo para o divisor d, será também um resíduo para o divisor $4nq+d$, mas um não-resíduo para o divisor $4nq-d$.

346. Se o número positivo n for um resíduo para o divisor d, e também para o divisor e, será ainda um resíduo para qualquer divisor primo da forma $4nq \pm de$. E se o número negativo $-n$ for um resíduo para os divisores d e e, será também um resíduo para qualquer divisor primo da forma $4nq+de$; mas para os divisores $4nq-de$ será achado entre os não-resíduos.

347. Se o número positivo n for um não-resíduo para os divisores d e e, certamente será um resíduo para todos os divisores primos da forma $4nq \pm de$; e se o número negativo $-n$ for um não-resíduo para os divisores d e e, será um resíduo para todos os divisores primos da forma $4nq+de$; mas para divisores da forma $4nq-de$ será um não-resíduo.

348. Seja proposto qualquer número $\pm n$; ele sempre será um resíduo, se o divisor primo for contido em alguma das

seguintes formas: $4nq+A$, $4nq+B$, $4nq+C$, *etc*., cuja quantidade é igual à metade da quantidade de números que são primos com $4n$ e menor que ele. Mas se o divisor for contido nas formas restantes, será um não-resíduo.

349. Os casos em que o número n é um quadrado devem ser colocados à parte, pois um quadrado sempre ocorrerá entre os resíduos, qualquer que seja o divisor. Mas, se n for um quadrado negativo, valerá o mesmo raciocínio quanto o usado para -1.

350. Deve ser demonstrado[24] em primeiro lugar, portanto, a proposição de que, se o divisor primo for $4nq+ii$, sendo i um número ímpar, tanto os números n e q, quanto seus negativos $-n$ e $-q$, sempre ocorrerão entre os resíduos. Seja $i = 2m+1$ e, porque o divisor $4nq+4mm+4m+1$ é da forma $4p+1$, o quadrado negativo $-4mm-4m-1$ será contido entre os resíduos[25] e, porque os números $4nq$ e 4 são resíduos, também o número nq, bem como $-nq$ serão resíduos; em consequência, ambos os números n e q deverão ocorrer ao mesmo tempo entre os resíduos, ou ao mesmo tempo entre os não-resíduos; logo,

[24] N. do Trad. Isto é, a primeira proposição relacionada em §344 como não demonstrada. Observe que a demonstração de Euler não é completa.
[25] N. do Trad. Ver §333 e, para as próximas consequências, §318 ($4nq$ é o complemento do quadrado negativo) e §307.

quando um ou outro estiver entre os resíduos, será necessário que o outro seja achado na mesma classe.

351. Se n não fosse um resíduo, não haveria quadrado xx algum, tal que $xx-n$ é divisível por $4nq+4mm+4m+1$. Logo, se puder ser demonstrado que há algum quadrado do referido tipo, a verdade da proposição será estabelecida. De fato, se n fosse um não-resíduo, a expressão $n^{2nq+2mm+2m}-1$ não seria divisível pelo número primo e, por isto, se o contrário pode ser demonstrado, teremos o que precisamos. (*)

(*) *Escrito na margem*: Se n fosse um não-resíduo, nzz seria algum não-resíduo e, portanto, também

$$\pm nxx\mp y(4nq+4mm+4m+1),$$

qual expressão, se fosse um quadrado em pelo menos um caso, validaria a proposição. Mas, na verdade, devido aos sinais ambíguos, parece que isto deve sempre acontecer em pelo menos um caso; e é ainda mais verdadeiro, visto que n e q são permutáveis, mesmo que o divisor não seja primo. Questão, se $n = 3$, $q = 5$, $2m+1 = 5$, $\pm 3zz \pm 85y$, ou $\pm 5zz \pm 85y$ não pode ser feito um quadrado. A demonstração deveria ser elaborada de tal forma que o divisor seja primo.

352. Agora, é necessário demonstrar[26] que, se o divisor primo for $4nq-4mm-4m-1$, o número n ocorrerá entre os resíduos dos quadrados, mas o número $-n$ entre os não-resíduos. Igualmente, o número q estará entre os resíduos e $-q$ entre os não-resíduos. Mas, visto que $(2m+1)^2$ certamente está entre os resíduos, $4nq$ estará na mesma classe e, portanto, também nq.

353. Aceitando essas proposições, embora ainda não fossem demonstradas, sejam i um número ímpar e $4nq \pm ii$ primo; para o divisor primo $4nq+ii$, visto que n e $-n$ são resíduos, bem como naa e $-naa$, sempre haverá algum quadrado xx, tal que $xx-naa$ seja divisível por $4nq+ii$, e ainda algum quadrado yy, tal que $yy+naa$ seja divisível por $4nq+ii$.

354. Mas, sendo $4nq-ii$ o divisor primo, devido ao fato de que naa é resíduo, sempre haverá um quadrado xx, tal que $xx-naa$ seja divisível por $4nq-ii$; não há, porém, um quadrado yy algum, que faz com que $yy+naa$ seja divisível por $4nq-ii$, pois neste caso $-naa$ é um não-resíduo.

355. Como $4nq+ii$ é um número da forma[27] $4p+1$, sempre haverá uma soma de dois quadrados $ff+gg$ que é divisível por ele, dos quais um ff pode ser tomado à vontade. Em

[26] N. do Trad. Isto é, a segunda proposição enunciada em §344. De novo, a demonstração é incompleto, o que Euler reconhece no próximo parágrafo.
[27] N. do Trad. Todo quadrado ímpar tem a forma $4q+1$. Ver também §334 e a nota de Euler.

consequência, se $xx–naa$ é divisível por $4nq+ii$, um quadrado yy pode ser encontrado, que faz com que $xx+yy$ seja divisível por $4nq+ii$ e, então, também $yy+naa$ será divisível pelo mesmo divisor.

356. Como $4nq–ii$ tem a forma $4p–1$, não[28] haverá soma alguma de quadrados divisível por $4nq–ii$; em consequência, se $xx–naa$ for divisível por $4nq–ii$, não será possível fazer com que $yy+naa$ seja divisível pelo referido divisor; pois, também a soma $xx+yy$ seria divisível, o que é absurdo.

357. Tomando $d = 4nq+ii$ como o divisor primo, visto que a forma $xx+naa$ é divisível por ele, também a forma $yy+qaa$ será divisível por ele, bem como, portanto, a forma $qxx–nyy$. Acontecerá, então, que também a forma $yy–qaa$ é divisível e, por causa disto, qualquer soma da forma $qxx+nyy$.

358. Se o divisor primo for $d = 4nq–ii$, visto que as fórmulas $xx–naa$, bem como $yy–qaa$, são por ele divisíveis, também a forma $qxx–nyy$ será divisível por d. No entanto, como a forma $yy+qaa$ não é divisível por d, nenhuma forma $qxx+nyy$ será divisível por d.

359. Na verdade, embora essas proposições possem ser demonstradas, as outras, como observamos acima, ainda não foram estabelecidas. Do §345, há um quadrado, deixando um

[28] N. do Trad. Ver §337 e a nota de Euler.

resíduo positivo n quando dividido por d – de fato, há um deixando naa; mas, então, sendo $4nq \pm d$ um número primo, há um quadrado xx, que, dividido por $4nq \pm d$, deixa o mesmo resíduo, ou seja, $xx - naa$ será divisível por $4nq + d$.

360. Se, por exemplo, $bb - naa$ for divisível por d, o número $xx - naa$ sempre será divisível pelo número primo $4nq \pm d$. Mas, sendo i um número ímpar, podemos ainda exibir a forma $xx - naa$, que será divisível pelo número primo $4nq \pm dii$.

361. Se tiver um quadrado bb, que deixa um resíduo negativo $-n$, ou $-naa$, quando dividido por d, haverá também um quadrado xx, que, dividido pelo número primo $4nq + dii$, deixa o resíduo $-n$, ou $-naa$. Se, por exemplo, o divisor d for da forma $bb + ncc$, haverá um x, tal que $xx + naa$ é divisível pelo número primo $4nq + dii$.

362. De fato, se o divisor d for da forma $bb + ncc$, não haverá forma alguma $xx + naa$, que seja divisível pelo primo $4nq - dii$. Desta maneira, se tivermos $n = 3$, tomamos $d = 7$, porque $2^2 + 3 \cdot 1 = 7$, e, de fato, é certo que nenhum número da forma $xx + 3aa$ admite divisores da forma $12q - 7ii$, alguns dos quais são: 5, 17, 29, 41, 53, 65, 77, 89, 101, 9, 21, 33, 45.

363. De §346, segue que, se d e e forem divisores de certos números da forma $aa - nbb$, então sempre haverá um quadrado xx, tal que $xx - ncc$ seja divisível pelo número primo $4nq \pm deii$, o que, de fato, pode ser deduzido do precedente, ao

demonstrar que, se *aa–nbb* tiver o divisor *d*, e uma outra forma semelhante *ff–ngg* tiver o divisor *e*, então *hh–nkk* será divisível pelo produto *de*. Isto será claro se considerarmos resíduos de quadrados divididos por números compostos.

364. Ainda mais, merece ser observado que, o número *n* e, portanto, também *naa*, não pode ocorrer entre os resíduos de quadrados, a não ser que o divisor primo seja da forma $4nq+\alpha$, onde α não significa todos os números primos com $4a$ e menores que o mesmo, mas apenas metade deles, sendo a outra metade completamente excluída. E, assim, todos os divisores primos da forma *xx–naa* têm a forma $4nq+\alpha$, onde α denota vários números, sendo o mesmo tanto excluído.

365. O cálculo é semelhante para números da forma *xx+naa*, cujos divisores primos são compreendidos pela forma $4nq+\alpha$, de tal forma que a quantidade de números excluídos de α é a mesma da quantidade de números admitidos. Em qualquer caso, todo quadrado ímpar *ii* é válido para α e, se α for válido, também αii será válido.

366. Para trabalhar essas demonstrações que faltam, consideremos divisores primos $4p+1$ e, visto que se pode exibir uma soma *aa+bb* de dois quadrados, divisível pelo referido divisor, tal que um pode ser tomado à vontade, $(4p+1)bb$ é removido e $aa–4pbb$ será divisível por $4p+1$, ou seja, há um

quadrado *aa*, que deixa o resíduo 4*pbb* quando dividido por 4*p*+1, portanto deixando *p*, ou seja, há uma forma *aa–pbb* divisível por 4*p*+1.

367. Visto que haja uma forma *aa–bb* divisível por 4*p*+1, somando (4*p*+1)*bb*, há também a forma *aa*+*pbb* divisível por 4*p*+1, o que já é claro, mas se os quadrados são divididos pelo número primo 4*p*+1, tanto +*p* quanto –*p* serão achados nos resíduos.

368. Seja, então, 4*ffp*+*ii* o divisor primo, sendo *i* um número ímpar, e porque pode-se exibir tanto a forma *aa*+*bb*, quanto *aa–bb*, divisíveis pelo referido divisor, também *iiaa*+*iibb* e *iiaa–iibb* serão divisíveis; subtraindo e depois somando (4*ffp*+*ii*)*bb*, teremos que as fórmulas *iiaa–*4*ffpbb* e *iiaa*+4*ffpbb* são divisíveis por 4*ffp*+*ii*, ou seja, ±4*ffpbb* estarão entre os resíduos dos quadrados e, portanto, também ±*p*. Haverá, portanto, números tanto da forma *xx*+*pyy*, quanto da forma *xx–pyy* que são divisíveis por 4*ffp*+*ii*. (*)

(*) *Escrito na margem*: O primeiro claramente; pois $\frac{xx + pyy}{4\,ffp + ii}$ = inteiro, se $x = i$, $y = 2f$;

para $xx–2yy$ ser divisível por 41, $x = 7, 10, 13, 14, 17$
$y = 2, 3, 8, 4, 1$

para $xx–2yy$ ser divisível por 17,

$x =$	12, 5	11, 6	10, 7	16, 1	17, 4
$y =$	2	1	4	3	5

369. Se, aceitando as observações feitas acima, o divisor primo for contido em qualquer dessas fórmulas: $4rq+1$, $4rq+\alpha$, $4rq+\beta$, $4rq+\gamma$, $4rq+\delta$, *etc*., onde os números 1, α, β, γ, δ, *etc*. são primos com $4r$ e menores que ele, dos quais, contudo, ocorrem só a metade, então o número r certamente ocorrerá entre os resíduos dos quadrados; e as fórmulas dos divisores para o resíduo $-r$ são analisadas de modo semelhante, sendo que concordam com estas quando o divisor tem a forma $4p+1$, e divergem quando o divisor tem a forma $4p-1$.

370. Merece ser observado que, das formas $4rq+4m+1$, metade é excluído tanto para o resíduo $+r$, quanto para $-r$, cujos divisores para essa forma são comuns. Mas, da forma $4rq+4m-1$, metade vale para o resíduo $+r$ e a outra metade para o resíduo $-r$ e, aqui, os divisores que valem para um resíduo são excluídos do outro.

Capítulo XI

Sobre resíduos surgidos da divisão de cubos por números primos

371. Sendo $d = 2p+1$ um divisor primo, qualquer que seja o resíduo deixado pelo cubo a^3, o mesmo será deixado pelos cubos $(a+d)^3$, $(a+2d)^3$, *etc*. e, em geral, $(a+nd)^3$; por isso, será suficiente considerar os cubos, cujas raízes são menores que d, a saber,

$$1, 8, 27, 64, ..., (d-4)^3, (d-3)^3, (d-2)^3, (d-1)^3.$$

372. Seja r o resíduo que um cubo qualquer, a^3, deixa; então é claro que o cubo $(d-a)^3$ deve deixar o resíduo $-r$, ou seja, $d-r$. Assim, se um número qualquer r ocorrer entre os resíduos dos cubos, seu simétrico $-r$, ou seja $d-r$, o que é chamado seu complemento, ocorrerá no mesmo lugar.

373. Sejam 1, α, β, γ, δ, *etc*., os resíduos surgidos da divisão dos cubos por um número primo $d = 2p+1$. Se todos eles forem mutuamente distintos, sua quantidade será $= d-1$ e, portanto, todos os números menores que d ocorrerão entre os resíduos. Mas, se uns números ocorrerem duas ou mais vezes, então certamente uns números serão excluídos, sendo eles incluídos entre os não-resíduos.

(*) Todos os cubos menores que d^3 ocorrerão entre esses resíduos, bem como os produtos, reduzidos aos valores mínimos, de dois, três, *etc*., deles.

374. Querendo investigar se é possível que um mesmo número r ocorresse entre os resíduos duas vezes, suponhamos que o mesmo resíduo r resulta dos cubos a^3 e b^3, cujas raízes a e b são números distintos, menores que o divisor d. Assim, sua diferença $b^3–a^3 = (b–a)(aa+ab+bb)$ será divisível por d. Visto que d é primo e o fator $b–a$ é primo ao mesmo, é necessário que o outro fator $aa+ab+bb$ seja divisível por d.

375. E se o cubo b^3 fornecer o mesmo resíduo que a^3, a qualquer outro cubo c^3 corresponderá algum cubo e^3, deixando o mesmo resíduo. Pois, se os cubos a^3 e b^3 fornecem o mesmo resíduo, também a^3x^3 e b^3x^3, reduzidos aos valores mínimos, isto é, $(ax–md)^3$ e $(bx–nd)^3$, produzirão o mesmo resíduo. Visto que a e d são primos entre si, sempre se pode achar x e m tais que $ax–md$ seja igual ao dado número c. Em consequência, teremos que $e = bx–nd$ é distinto de c e menor que d, pois se tivéssemos $e = c$, teríamos $ax–md = bx–nd$ e, portanto, $(a–b)x$ seria divisível por d embora nem $a–b$ nem x é divisível.[1]

376. Portanto, se um resíduo ocorrer duas vezes, segue imediatamente que todos ocorrerão duas vezes e, assim, a

[1] N. do Trad. $d \mid x \Rightarrow d \mid (ax–md) = c$, o que é contra a hipótese de que $c < d$.

quantidade de resíduos distintos será reduzida pela metade. Isto não pode acontecer, porém, a não ser[2] que o divisor d seja um divisor da forma $aa+ab+bb$, sendo a e b menores que d. Mas, se o divisor não for da referida forma, todos os resíduos serão distintos e a quantidade deles será $= d-1 = 2p$.

377. Sejam, então, a^3 e b^3 cubos que fornecem o mesmo resíduo, de tal forma que a^2+ab+b^2 seja divisível por d. Assim, $3a^3+3a^2b+3ab^2$ será divisível por d e, subtraendo a^3-b^3, teremos que

$$2a^3+3a^2b+3ab^2+b^3 = a^3+(a+b)^3$$

será divisível por d. Porque a^3 deixa r, o cubo $(a+b)^3$ deixará $-r$ e, portanto[3], o cubo $(d-a-b)^3$, ou $(2d-a-b)^3$, dará o resíduo $+r$.

378. É imediato, portanto, que, se houver dois cubos a^3 e b^3 que deixam o mesmo resíduo r, haverá um terceiro $(d-a-b)^3$, ou $(2d-a-b)^3$, que também deixa o mesmo resíduo; sua raiz será menor que d e distinta de ambas as precedentes, a e b. De fato, não podemos ter $d-a-b = a$, nem $2d-a-b = a$; pois, se tivéssemos $b = d-2a$, ou $b = 2d-2a$, então b^3 deixaria o resíduo $-8a^3$, ou seja, $-8r$. Mas, visto que deixa o resíduo r por hipótese e porque esses dois resíduos r e $-8r$ não podem ser equivalentes (pois sua diferença $= 9r$ não é divisível por d, exceto no caso em

[2] N. do Trad. Ver §374.
[3] N. do Trad. Ver §372.

que $d = 3$, que é um caso transparente[4]), segue que, havendo dois resíduos iguais, sempre terá um terceiro igual.

379. Se, portanto, dois cubos a^3 e b^3 fornecerem o mesmo resíduo r, haverá, por essa mesma razão, um terceiro c^3, exibindo o mesmo resíduo, cuja raiz é constituída de tal forma que a soma de todas $a+b+c$ será ou $= d$, ou $= 2d$, pois $c = d–a–b$, ou $c = 2d–a–b$, cada um sendo menor que d. E, assim, o terceiro é facilmente achado a partir de dois.

380. Pode-se deduzir disso, porém, que nunca haverá mais que três cubos a^3, b^3, c^3, menores que d^3, que deixam o mesmo resíduo. Pois, se houvesse um quarto e^3, distinto daqueles, os seguintes também forneceriam o mesmo resíduo[5]:

$$(\lambda d–a–e)^3, \quad (\lambda d–b–e)^3, \quad (\lambda d–c–e)^3$$

e eles seriam distintos dos precedentes. Pois, se tivesse $\lambda d–a–e = b$, então $a+b+e$ seria divisível por d e, portanto, $e = c$, contra a hipótese; teríamos não somente quatro, mas sete cubos dando o mesmo resíduo.

381. Desta forma, por combiná-los dois a dois, mais cubos podem ser achados, menores que d^3, que também deixam resíduos, até todos os cubos aparecem. Com um resíduo dado r,

[4] N. do Trad. No caso de $d = 3$, há $d–1$ resíduos distintos, a saber, 1 e –1. Observamos ainda que, no texto original, o presente parágrafo é numerado 387, erroneamente.
[5] N. do Trad. Em cada caso, $\lambda = 1$ ou $\lambda = 2$.

um outro –r é achado, e é claro que não há mais que três cubos, menores que d^3, que exibem o mesmo resíduo.[6]

382. Portanto, na série dos resíduos1, α, β, γ, *etc*., cuja quantidade é = $d-1 = 2p$, ou são todos distintos, ou são iguais de três em três[7]. Mas, o segundo caso não pode acontecer, a menos que $2p$ seja um número divisível por 3. Por isto, se p não for divisível por 3, é certo que todos os resíduos serão distintos e, portanto, todos os números menores que d ocorrerão entre os resíduos.

383. Visto que cada número primo, exceto 2 e 3, é contido em uma ou outra[8] das formas $6q+1$ e $6q-1$, se o divisor primo for $6q-1$, todos os números menores que o referido divisor ocorrerão entre os resíduos e não haverá não-resíduos. Se, porém, o divisor for $6q+1$, será possível que a quantidade de resíduos distintos seja apenas $2q$ e, assim, haverá $4q$ não-resíduos.

384. Vimos[9], porém, que esse último caso acontece se o divisor for da forma $aa+ab+bb$; disto é claro que, como já

[6] N. do Trad. O pensamento de Euler neste parágrafo não é inteiramente claro. Parece que ele está afirmando que, visto que há mais de três maneiras de combinar dois resíduos (incluindo suas potências), basta descobrir dois resíduos para poder calcular todos os outros. De fato, ele continua, basta descobrir um, pois seu simétrico também será um resíduo. Compare isto com §388.

[7] N. do Trad. Na há implicação de qualquer tipo de ordem aqui; a afirmação é apenas que cada resíduo distinto aparece três vezes na série.

[8] N. do Trad. $6q$, $6q+2$ e $6q+4$ são divisíveis por dois, enquanto $6q+3$ é divisível por 3. Os números 2 e 3 são excluídos porque Euler não considerou a possibilidade de $q = 0$.

[9] N. do Trad. Ver §374.

observamos[10] acima, tal forma não admite outros divisores primos além dos da forma $6q+1$. Mais ainda, seu quádruplo $4aa+4ab+4bb = (2a+b)^2+3b^2$ se reduz à forma $aa+3bb$, cujos divisores primos gozam desta notável propriedade.[11]

385. Procuramos, então, primos que são divisores de quadrados, deixando como resíduo ou -3 ou $-3bb$, que, como observado acima (§341), são contidos nas duas fórmulas $12q+1$ e $12q+7$, o que se reduz à forma única $6q+1$. Disto pode-se concluir, por sua vez, que todos os números primos da forma $6q+1$ são dotados dessa propriedade, embora ainda falte uma demonstração plena dessa coisa até agora.

386. Dado isto, porém, obtemos a seguinte proposição: Sempre que o divisor primo for da forma $6q+1$, nem todos os resíduos dos cubos[12] de 1 a $216q^3$ serão distintos, mas, porque serão iguais em trios, a quantidade de resíduos distintos será apenas $2q$ e o restante dos números menores que o divisor, cuja quantidade é $4q$, serão não-resíduos. Sempre que o divisor primo não for da forma $6q+1$, porém, todos os resíduos serão distintos e não haverá não-resíduos.

---

[10] N. do Trad. Na nota (*) ao §272, Euler observa que só primos da forma $3\lambda+1$ dividem a referida forma e claramente nenhum número da forma $3\lambda+1$ é da forma $6q-1$.

[11] N. do Trad. Ver §402. Observe que, se $a^2+3b^2 = qd$, então $a^2 = qd-3b^2$ e, assim, $-3b^2$ é o resto da divisão de a^2 por d (ou, como diríamos hoje, é equivalente a esse resto).

[12] N. do Trad. Isto é, os $6q$ cubos (positivos) cujas raízes são menores do divisor $d = 6q+1$. Para a demonstração de Euler da primeira proposição, ver §397 e §398.

387. Precisa-se considerar, portanto, apenas divisores primos da forma $6q+1$, para os quais a quantidade dos não-resíduos é o dobro da dos resíduos. Apresentaremos os casos mais simples:

para o divisor:	7	13	19
resíduos:	1, 6	1, 8, 5, 12	1, 8, 7, 11, 12, 18
não-resíduos:	2, 3	2, 4, 3, 6	2, 3, 4, 5, 6, 9
	5, 4	11, 9, 10, 7	17, 16, 15, 14, 13, 10

para o divisor:	31
resíduos:	1, 8, 27, 2, 16, 15, 29, 4, 23, 30
não-resíduos:	3, 5, 6, 7, 9, 10, 11, 12, 13, 14
	28, 26, 25, 24, 22, 21, 20, 19, 18, 17

para o divisor:	37
resíduos:	1, 8, 27, 14, 31, 10, 6, 23, 29, 11, 26, 36
não-resíduos:	2, 3, 4, 5, 7, 9, 12, 13, 15, 16, 17, 18
	35, 34, 33, 32, 30, 28, 25, 24, 22, 21, 20, 19

para o divisor:	43
resíduos:	1, 8, 27, 21, 39, 11, 4, 32, 22, 16, 35, 2, 41, 42
não-resíduos:	3, 5, 6, 7, 9, 10, 12, 13 ,14, 15, 17, 18, 19, 20
	40, 38, 37, 36, 34, 33, 31, 30, 29, 28, 26, 25, 24, 23

388. Para qualquer divisor primo da forma $6q+1$, portanto, todos os cubos menores que o divisor ocorrem entre os resíduos, bem como seus complementos[13] $6q$, $6q-7$, $6q-26$, $6q-63$, *etc*. Continuando, ocorrem também seus produtos dois a dois. Então é também verdadeiro que, se qualquer produto mn,

[13] N. do Trad. Ver §372.

junto com um dos fatores m, estiveram entre os resíduos, também o outro fator n será achado no mesmo lugar.

389. Pois, se a^3 deixa mn e b^3 deixa m, para o divisor $6q+1 = d$, pode-se colocar[14] $a = fb–gd$ e, portanto, f^3b^3 deixa mn, e também nb^3 deixa mn e, assim, $f^3b^3–nb^3$ e logo $f^3–n$ será divisível por d, ou seja, f^3 deixará n.

390. Se o número α ocorrer entre os resíduos dos cubos, sendo $d = 6q+1$ o divisor primo, então $\alpha^{2q}–1$ será divisível[15] por d. Em consequência, os resíduos que surgem da divisão da progressão geométrica $1, \alpha, \alpha^2, \alpha^3, \alpha^4, ..., \alpha^{2q}$ pelo mesmo divisor, concordam com os resíduos dos cubos.

391. Por sua vez, deve ser mostrado que, se $a^{2q}–1$ for divisível pelo divisor primo $6q+1$, o número a certamente ocorrerá entre os resíduos dos cubos, o que é fácil quando $2q$ não é divisível por 3. Pois, se $2q = 3k\pm1$, como $a^{2q} = a^{3k\pm1}$ ocorre entre os resíduos, visto que é equivalente à unidade, a^{3k} de fato estará no mesmo lugar e será necessário que a seja achado no mesmo lugar.[16]

392. Resta, portanto, mostrar que, se $2q = 3k$ e $a^{3k}–1$ puder ser dividido por $6q+1 = 9k+1$, então a estará entre os

[14] N. do Trad. Por hipótese, $b < d$, com d primo; logo b e d são coprimos. Ver a nota de Euler ao §139.
[15] N. do Trad. Se α é resíduo, há algum a tal que, módulo d, $\alpha \equiv a^3$; assim, $\alpha^{2q} \equiv a^{6q} \equiv 1$, pois $6q = \varphi(d)$.
[16] N. do Trad. Ver §388.

resíduos dos cubos (*); a^{3k} com certeza será achado no referido lugar, visto que é um cubo, mas ainda deve ser demonstrado que o resíduo de a^{3k} seja equivalente à unidade.

(*) Escrito na margem: Pois, se a fosse um não-resíduo, todos os outros não-resíduos, que são a, $a\alpha$, $a\beta$, $a\gamma$, $a\delta$ e a^2, $a^2\alpha$, $a^2\beta$, $a^2\gamma$, *etc*. gozariam da mesma propriedade, de tal forma que suas potências ao expoente $2q$, menos a unidade, seriam divisíveis por $6q+1$; portanto, todos os números teriam essa propriedade, o que é absurdo.

393. De fato, como os resíduos das potências 1 a, a^2, a^3, *etc*., em quantidade de $2q$, como os resíduos dos cubos, são distintos, e porque ambas as classes começam com a unidade e têm os termos a^3, a^6, a^9, *etc*. em comum, então as outras propriedades são comuns e a classe de potências não pode conter termos diferentes da outra classe.

394. Consideremos os não-resíduos de cubos, divididos pelo número primo $6q+1$; com certeza, se mn for um resíduo e m um não-resíduo, também n será um não-resíduo. Por outro lado, nem todos os produtos de dois não-resíduos fornecerão um resíduo; mas todo produto de qualquer resíduo com um não-resíduo será um não-resíduo[17].

[17] N. do Trad. Ver §387, onde em relação a $d = 13$, por exemplo, o produto de não resíduos $2\times4 = 8$, um resíduo, enquanto o produto dos não-resíduos $2\times3 = 6$, um não resíduo.

395. Em primeiro lugar, os quadrados dos vários não-resíduos são contidos entre os não-resíduos; isto é, se A for um não-resíduo, A^2 também será um não-resíduo, mas se esse não-resíduo A^2 for multiplicado pelo não-resíduo A, certamente dará um resíduo, pois é um cubo.

396. Pois, se A^2 fosse um resíduo, $A^{4q}-1$ seria[18] divisível por $6q+1$; e como $A^{6q}-1$ certamente é divisível, também seria $A^{6q}-A^{4q}$, isto é, $A^{2q}-1$ seria divisível e, portanto, A seria o resíduo de um cubo, contra a hipótese. Por isto, se AA for um resíduo, A também será um resíduo e, ao contrário[19], se A for um não-resíduo, AA também será um não-resíduo.

397. Portanto, se o divisor primo for $= 6q+1$, os resíduos dos cubos forem $1, \alpha, \beta, \gamma, \delta$, *etc*, e se tivermos um único não-resíduo A, então, em primeiro lugar, todos os números A, $A\alpha$, $A\beta$, $A\gamma$, *etc*. e, depois, esses A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc*. serão não-resíduos. É claro que, visto que são todos mutuamente distintos, a quantidade desses números, como agora demonstramos, é duas vezes a quantidade dos resíduos.

398. Disto, é claro que, se o divisor primo for $6q+1$, pode haver somente $2q$ resíduos distintos; pois, se todos os números ocorressem entre os resíduos, $a^{2q}-1$ seria[20] em geral divisível

[18] N. do Trad. Ver §390.
[19] N. do Trad. Isto é, a contraposição.
[20] N. do Trad. Ver, mais uma vez, §390.

por $6q+1$, qualquer que seja $a < 6q+1$; mas, porque isto é absurdo, há pelo menos um não-resíduo e, disto mesmo, segue que há $4q$ não-resíduos.

399. Assim, visto que a partir de um único não-resíduo A se obtém duas classes de não-resíduos, sendo a primeira A, $A\alpha$, $A\beta$, $A\gamma$, *etc*. e a segunda A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc*., cada uma contendo a mesma quantidade de termos quanto a classe dos resíduos, o produto de dois de uma das classes será achado na outra classe e o produto de dois de classes diferentes será[21] um resíduo.

400. Duvidemos, mesmo agora, se todos os não-resíduos sejam de fato obtidos desta maneira a partir de um único não-resíduo? Seja B um não-resíduo não contido em qualquer uma das duas classes. Então tanto B, $B\alpha$, $B\beta$, $B\gamma$, *etc*., quanto B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc*. serão não-resíduos, tendo cada grupo a mesma quantidade de termos quanto há de resíduos, e todos esses números serão distintos dos precedentes[22]. Mais ainda, ou AB ou AB^2 não será um resíduo; certamente um será um resíduo e o outro um não-resíduo.

(*). *Escrito na margem*. Deve ser demonstrado que ambos não podem ser simultaneamente não-resíduos. Se AB fosse um não-resíduo, seria contido

[21] N. do Trad. O produto, por exemplo, $A\alpha \times A^2\beta = A^3\alpha\beta$, o produto de três resíduos e, portanto, é um resíduo. Os outros casos são semelhantes.

[22] N. do Trad. Se $B\alpha$ estivesse numa das séries A ou A^2, $B\alpha$, $(B\alpha)\alpha$, $(B\alpha)\beta$, ..., $(B\alpha)^2$, $(B\alpha)^2\alpha$, ... seriam os não-resíduos originais e, portanto, B estaria numa dessa séries originais (há algum $\gamma\delta = 1$), contra a hipótese.

na classe ou de A, ou de B, ou de A^2, ou de B^2. Mas, cada um é um absurdo e, portanto, AB é um resíduo.

401. Se AB não fosse um resíduo, poderíamos representar duas classes de não-resíduos assim:

Primeira classe: A, $A\alpha$, $A\beta$, $A\gamma$, *etc*. B, $B\alpha$, $B\beta$, $B\gamma$, *etc*.

Segunda classe: A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc*. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc*.

e um número qualquer da primeira classe de A, multiplicado por qualquer um da segunda classe, forneceria um resíduo e ele certamente seria distinto de qualquer um que seja. Em consequência, mais resíduos seriam produzidos que de fato há, o que é absurdo.

402. Logo, visto que há apenas $2q$ resíduos para o divisor primo $6q+1$, dado um cubo a^3 qualquer, há um outro b^3, menor que $(6q+1)^3$, tal que a sua diferença é divisível por $6q+1$ e, assim, $aa+ab+bb$ será divisível pelo mesmo número. Todo número primo $6q+1$ é, portanto, divisor[23] de algum número $aa+3bb$, ou algum $aa+3$ ou algum $3aa+1$.

[23] N. do Trad. Ver §384 e §385.

403. Pondo 373 no lugar do divisor, teremos os seguintes resíduos dos cubos, bem como os não-resíduos das duas classes[24]:

Resíduos	Não-resíduos	
±	De Classe I. ±	De Classe II. ±
1, 7, 8, 12, 13, 17	2, 3, 5, 14, 16, 21	4, 6, 9, 10, 11, 15
18, 19, 20, 22, 23	24, 26, 34, 35, 36	25, 28, 29, 32, 37
27, 30, 31, 33, 41	38, 39, 40, 44, 46	42, 43, 48, 52, 63
45, 49, 50, 55, 56	47, 51, 53, 54, 57	68, 70, 71, 72, 73
58, 64, 67, 74, 75	59, 60, 61, 62, 65	76, 77, 78, 79, 80
84, 86, 87, 91, 96	66, 69, 81, 82, 83	88, 92, 94, 102, 103
97, 104, 109, 111, 113	85, 89, 90, 93, 95	105, 106, 108, 114, 117
119, 125, 126, 129, 133	98, 99, 100, 101, 107	118, 120, 122, 124, 127
136, 137, 139, 140, 142	110, 112, 115, 116, 121	130, 131, 132, 138, 141
144, 145, 146, 152, 154	123, 128, 134, 135, 147	143, 149, 153, 159, 162
156, 157, 158, 160, 161	148, 150, 151, 155, 165	164, 166, 170, 171, 173
163, 167, 169, 176, 184	168, 172, 174, 179, 181	175, 177, 178, 180, 183
185.	182.	186.
quantidade 2·62 = 124.	quantidade = 124.	quantidade = 124.

404. Visto que o divisor primo é $6q+1$ e a quantidade de não-resíduos é o dobro da quantidade de resíduos, haverá menos

[24] N. do Trad. Observe que cada número na tabela representa se mesmo e seu simétrico. Assim, temos, por exemplo, 7 e –7 (ou seja, 366).

divisores para os quais um dado número será contido entre os resíduos. Assim, um dado número a será um resíduo, si o divisor for um fator da forma $x^3 \pm ay^3$, ou da forma $x^3 \pm aay^3$; pois, se $x^3 \pm ay^3 = dn$, o cubo x^3, dividido por d, dará ay^3 e a estará entre os resíduos.[25]

405. Procura-se, portanto, os divisores primos dos números[26] $x^3 \pm ay^3$ e se escolha apenas os que são simultaneamente da forma $6q+1$. Desta forma, pondo, $a = 2$, dois será achado entre os resíduos, sempre que o divisor da forma $6q+1$ estiver um número da seguinte série:
31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997, 1021, 1051, 1069, 1093, *etc*.

406. Seja, então, $6n+1$ um número, tal que tanto 2, quanto 2^2, são resíduos. Assim[27], $2^{2n}-1$ será divisível pelo mesmo e, portanto, ou 2^n-1 ou 2^n+1. Mas, se $6n+1$ for ou da forma $8m+1$, ou $8m+7$, isto é, ou $n = 4m$, ou $n = 4m+1$, então também $2^{3n}-1$ será divisível por $6n+1$. Em consequência, é claro que nos casos em que n é ou $4m$ ou $4m+1$, teremos que 2^n-1 é divisível por $6n+1$, enquanto nos casos em que n é ou $4m+2$ ou $4m+3$, não 2^n-1, mas 2^n+1 será divisível por $6n+1$.

[25] N. do Trad. Ver §388.
[26] N. do Trad. Às vezes é mais fácil achar um divisor de $x^3 \pm a^2y^3$. Nesse caso, a^2 será um resíduo e, portanto (por §396), a também será resíduo.
[27] N. do Trad. Ver §396.

407. Assim, transferindo para cá os números dados acima, temos[28]:

por	é divisível	por	é divisível
31	$2^{10}-1$ e $2^{5}-1$	499	$2^{166}-1$ e $2^{83}+1$
43	$2^{14}-1$ « $2^{7}+1$	601	$2^{200}-1$ « $2^{100}-1$
109	$2^{36}-1$ « $2^{18}+1$	643	$2^{214}-1$ « $2^{107}+1$
127	$2^{42}-1$ « $2^{21}-1$	691	$2^{230}-1$ « $2^{115}+1$
157	$2^{52}-1$ « $2^{26}+1$	727	$2^{242}-1$ « $2^{121}-1$
223	$2^{74}-1$ « $2^{37}-1$	733	$2^{244}-1$ « $2^{122}+1$
229	$2^{76}-1$ « $2^{38}+1$	739	$2^{246}-1$ « $2^{123}+1$
277	$2^{92}-1$ « $2^{46}+1$	811	$2^{270}-1$ « $2^{135}+1$
283	$2^{94}-1$ « $2^{47}+1$	919	$2^{306}-1$ « $2^{153}-1$
307	$2^{102}-1$ « $2^{51}+1$	997	$2^{332}-1$ « $2^{166}+1$
397	$2^{132}-1$ « $2^{66}+1$	1021	$2^{340}-1$ « $2^{170}+1$
433	$2^{144}-1$ « $2^{72}-1$	1051	$2^{350}-1$ « $2^{175}+1$
439	$2^{146}-1$ « $2^{73}-1$	1069	$2^{356}-1$ « $2^{178}+1$
457	$2^{152}-1$ « $2^{76}-1$	1093	$2^{364}-1$ « $2^{182}+1$

408. Se considerarmos atentamente esses divisores, pelos quais 2 é feito um resíduo, observaremos[29] que todos eles

[28] N. do Trad. No original tem-se, na última entrada da primeira linha, $3^{83}+1$, o que é de fato divisível por 499, mas não parece obedecer ao padrão da tabela. Na sexta linha, tem-se $2^{122}-1$ para a última entrada; Isto é errado.

resultam da forma $27pp+qq$, sempre que o mesmo for um número primo, embora não se pode ainda confirmar essa observação por uma demonstração.

409. Se procurarmos os divisores primos $6q+1$, pelos quais 3 é feito um resíduo, acharemos:

61, 67, 73, 103, 193, 307, 367, 439, 577, 1021, *etc*.

os quais, se sejamos permitidos fazer uma conjectura, são contidos na forma $3pp+qq$, onde temos que ou $p = 9n$, ou $p \pm q = 9n$.

410. Os divisores primos da forma $6q+1$, que têm 5 entre os resíduos dos cubos, serão achados a partir da forma $x^3 \pm 5y^3$. Esses divisores devem ser 13, 67, 127, 181, 199, 241 487, 739, *etc*.; observamos que são contidos na forma $3pp+qq$ sob essas condições: 1) se $p = 15n$, 2) se $p = 3m$ e $q = 5n$, 3) se $p \pm q = 15n$ e 4) se $p \pm 2q = 15n$.

411. Se 6 deve ocorrer entre os resíduos, os divisores são[30]

7, 37, 139,163, 181, 241,307,337, 349,379, 631, 727, 751, 997, *etc*.

---

[29] N. do Trad. Para os cálculos numéricos referentes aos primos neste parágrafo, bem como os próximos, ver a Introdução.

[30] N. do Trad. A lista de Euler não é completa, pois, como também acontece com 307, o divisor primo 439 tem tanto 2, quanto 3, como resíduos e, assim, terá também 6 como resíduo. O referido divisor também satisfaz o critério eulerano, pois $439 = 3(9)^2+14^2$. De fato, módulo 439, temos $13^3 \equiv 2$, $87^3 \equiv 3$ e $241^3 \equiv 6$.

que serão contidos na forma $3pp+qq$, se tivermos ou $p = 9n$, ou $2p \pm q = 9n$. A verdade dessas observações, no entanto, teve seu início apenas por conjetura e, de fato, não podemos avançar, de forma cômoda, além deste ponto por indução.

(*) *Escrito na margem*. Para 7 ser um resíduo e o divisor $3pp+qq$, devemos ter ou $p = 3m$ e $q = 7n$, ou $p \pm q = 21n$, ou $4p \pm q = 7n$, ou $p = 21m$, ou $p \pm 2q = 7n$. — Para 10 ser resíduo, para o divisor $3pp+qq$, deve ter ou $p = 5n$, ou $q = 5n$.

Capítulo XII

Sobre resíduos surgidos da divisão de biquadrados por números primos

412. Seja d um divisor primo; qualquer que seja o resíduo deixado pelo biquadrado a^4, o mesmo será deixado, não somente pelos biquadrados $(d+a)^4$, $(2d+a)^4$, *etc*., mas também por $(d-a)^4$. Em consequência, se $d = 2p+1$, não pode haver mais que p resíduos distintos.

413. Se os resíduos forem 1, α, β, γ, δ, *etc*., cuja quantidade não pode ser maior que p, todo biquadrado, reduzido, é claro, à forma mínima, ocorrerá entre eles e, mais ainda, gozam da propriedade de que o produto de dois será achado entre os mesmos.

414. Esses resíduos, portanto, nascem dos biquadrados 1, 16, 81, 256, ..., p^4 e nos convém investigar diligentemente se, ou não, para um dado divisor primo, $2p+1$, todos são distintos.

415. E, em primeiro lugar, é óbvio que, se um ocorrer duas vezes, por exemplo, a partir dos biquadrados a^4 e b^4, então, porque b^4-a^4 será divisível por $d = 2p+1$, poderemos[1] fazer $b = md \pm na$ e, assim, $n^4a^4-a^4$ será divisível, assim como n^4-1. Desta

[1] N. do Trad. Isto é sempre possível, pois, pelas condições do problema, a e d são primos entre si.

forma, c^4 e n^4c^4 produzirão resíduos iguais e cada resíduo ocorrerá duas vezes[2].

416. Assim, se d for um divisor da fórmula b^4-a^4, onde a e b são menores que $\frac{1}{2}d$, visto que nem $b-a$, nem $b+a$ pode ser por ele dividido, e a fórmula b^2+a^2 for divisível, cada resíduo ocorrerá duas vezes. Se, ao contrário, ele não for fator de tal forma b^2+a^2, todos os resíduos serão distintos.

417. Mas, por §279, todo primo que divide a forma $bb+aa$ é contido na forma $4q+1$ e, por essa razão, se o divisor proposta for da forma $4q-1$, certamente haverá, a partir da divisão dos biquadrados, $2q-1$ resíduos distintos e o mesmo número de não-resíduos, não mais. Abordaremos esse caso primeiro.

418. Seja, então, $4q-1$ o divisor primo e sejam 1, α, β, γ, δ, *etc*. os resíduos distintos surgidos da divisão dos biquadrados; sua quantidade será $2q-1$ e teremos a mesma quantidade de não-resíduos, A, B, C, D, *etc*. Em primeiro lugar, é claro que, se A for um não-resíduo, também $A\alpha$, $A\beta$, $A\gamma$, *etc*. serão não-resíduos. Pois, se Aa^4 fosse um resíduo, surgido do biquadrado b^4, a forma b^4-Aa^4 seria divisível por d. Mas, temos que $b = ma\pm nd$ e, em

[2] N. do Trad. Observe que nc e c são distintos módulo d.

consequência, tanto $m^4a^4 - Aa^4$, quanto $m^4 - A$, seriam divisíveis por d; assim, m^4 deixaria A, contra a hipótese.

419. De fato, esta propriedade estende-se a todos os divisores[3], de tal forma que o produto de um resíduo e de um não-resíduo será sempre um não-resíduo. Mas, o produto de dois não-resíduos, AB, se o divisor primo seja $4q-1$, certamente é um resíduo; pois, se fosse um não-resíduo, seria equivalente a algum termo Aa^4, de tal forma que $Aa^4 - AB$ e, portanto, $a^4 - B$ seriam divisíveis por d, contra a hipótese.

420. Nesse caso, portanto, em que o divisor é $= 4q-1$, os resíduos dos biquadrados são munidos da mesma propriedade quanto os resíduos dos quadrados e, ainda mais, claramente concordam com estes para o mesmo divisor. Isto é, todo resíduo dos biquadrados é contido nos resíduos dos quadrados e, visto que tem a mesma quantidade, é inteiramente necessário que sejam os mesmos e, portanto, o que expusemos acima[4] sobre os resíduos e não-resíduos também vale aqui.

421. Agora seja o divisor primo $4q+1$ e sejam $1, \alpha, \beta, \gamma, \delta$, *etc*. os resíduos, todos os quais têm a propriedade[5] de que $\alpha^q - 1$ é divisível por $4q+1$. Esses resíduos também serão contidos

[3] N. do Trad. Isto é, não somente divisores primos da forma $4q-1$, mas também os da forma $4q+1$.
[4] N. do Trad. Capítulo X.
[5] N. do Trad. Pelo Critério de Euler (§321). Ver também o próximo parágrafo.

entre os resíduos dos quadrados para o mesmo divisor $4q+1$; mas, por sua vez, nem todos os resíduos dos quadrados serão ao mesmo tempo resíduos dos biquadrados, o que é mostrado na seguinte maneira.

422. Um resíduo qualquer dos quadrados pode ser representado por x^2, o que, se fosse um resíduo de um biquadrado, seria tal que $x^{2q}-1$ é divisível por $4q+1$, onde x denota um número qualquer menor que o divisor; com certeza, $1^{2q}-1$, $2^{2q}-1$, $3^{2q}-1$, $4^{2q}-1$, ..., $(2q)^{2q}-1$, poderiam então ser divididos por $4q+1$, o que não pode ser feito e, assim, nem todo quadrado ocorre entre os resíduos dos biquadrados.

423. Se x^2 não ocorrer entre os resíduos dos biquadrados, αx^2, βx^2, γx^2, δx^2, *etc*. também não ocorrerão no referido lugar, mas, visto que são resíduos de quadrados, é claro que, entre os resíduos dos quadrados, cuja quantidade é $2q$, há no mínimo tantos não-resíduos de biquadrados, quantos há de resíduos de biquadrados. Em consequência, é claro que a quantidade de resíduos de biquadrados será ou = q, ou ainda menor; no entanto, a segunda alternativa não pode ser.

424. Para explanar isto mais facilmente, examinaremos os divisores mais simples da forma $4q+1$ e consideremos tanto os resíduos, quanto os não-resíduos dos biquadrados:

para o divisor		5	13	17	29
resíduos		1	1,3, 9	1,413,16	1,16,23,24,20,7, 25
não-resíduos	{	2	2, 6, 5	3,12,5,14	2,3,17,19, 11,14,21
		4	4,12,10	9,2,15,8	4, 6, 5, 9, 22, 28,13
		3	8, 11,7	10,6,11,7	8,12,10,18,15,27,26

para o divisor		37
resíduos		1, 16, 9, 12, 33, 10, 26, 34, 7
não-resíduos	{	2, 32, 14, 31, 29, 15, 24, 20, 18
		4, 27, 28, 25, 21, 30, 11, 3, 36
		8, 17, 19, 13, 5, 23, 22, 6, 35

425. Destes exemplos, vemos que o número dos resíduos é = q, do qual já demonstramos que não pode ser maior. A quantidade dos não-resíduos é três vezes maior; separamos os mesmos em três classes, visto que os números de cada classe gozam de propriedades características.

426. Estas três classes podem ser mais apropriadamente constituídas da seguinte maneira: visto que há quadrados que não ocorrem entre os resíduos, seja xx um quadrado de tal tipo; então, com certeza nem x, nem x^3, podem ser achados entre os resíduos[6]. Portanto, se os resíduos forem 1, α, β, γ, δ, ε, *etc*., as três classes de não-resíduos serão:

I. $x, \alpha x, \beta x, \gamma x, \delta x$, *etc*.

II. $x^2, \alpha x^2, \beta x^2, \gamma x^2, \delta x^2$, *etc*.

III. $x^3, \alpha x^3, \beta x^3, \gamma x^3, \delta x^3$, *etc*.

[6] N. do Trad. Ver §423.

427. Cada classe contém tantos termos quanto há de resíduos e todos os termos dessas classes são mutuamente distintos. De fato, os termos de uma mesma classe são claramente distintos; a diversidade dos termos de classes diferentes será mostrada agora.

428. Se αx fosse equivalente ao βx^2, teríamos que $\beta x^2 - \alpha x$, e portanto $\beta x - \alpha$, fossem divisíveis por $4q+1$; em consequência, visto que α é um resíduo, βx, sendo equivalente ao mesmo, também seria um resíduo, que é absurdo. De forma semelhante, se αx, ou αx^2, fosse equivalente a βx^3, teríamos que $\alpha - \beta x^2$, ou $\alpha - \beta x$, fosse divisível por $4q+1$ e, portanto, βx^2, ou βx, pertenceria à classe dos resíduos, contra a hipótese.

429. Por isto, se o número de resíduos for $= n$, o número de não-resíduos será $3n$, ou pelo menos não será menor que $3n$. E, de fato, se todos os não-resíduos estiveram contidos nas referidas três classes, será necessário que a quantidade de resíduos e não-resíduos, tomados juntos, seja $= 4q$ e, portanto, $n = q$.

430. Sendo essas classes estruturadas como fizemos, é claro que o produto de dois não-resíduos tanto da primeira classe, quanto da terceira, será contido na segunda classe. Ora, o produto ou de dois termos da segunda classe, ou de um termo da primeira com um da terceira, produzirá um resíduo. Mas, o

produto de um termo da primeira classe com um da segunda será achado na terceira classe, enquanto o produto de um da segunda classe com um da terceira será achado na primeira.

431. Disto se entende que um número quadrado não pode ser achado na primeira classe, nem na terceira, pois, quando multiplicado por se mesmo, resulta num resíduo. Assim, apenas a segunda classe contém quadrados e, visto que os resíduos podem ser considerados quadrados, a quantidade de todos os quadrados é = $2n$.

432. Se a segunda classe, junta com a dos resíduos, compreenderem todos os quadrados, que podem ser considerados resíduos[7] distintos com respeito ao divisor $4q+1$, cuja quantidade é = $2q$, como vimos[8] nos resíduos dos quadrados, então, visto que $2n = 2q$ e, portanto, $4n = 4q$, todos os números menores que o próprio divisor serão contemplados e, assim, não poderá haver não-resíduo algum que não é contido em nossas três classes e teremos $n = q$.

433. Ora, se alguém ainda duvidar se todos os números, que não sejam resíduos, ocorram em nossas três classes de não-resíduos, essa dúvida será removida por mostrar que não há quadrado algum que é não-resíduo e que não é contido na

[7] N. do Trad. Isto é, resíduos de quadrados.
[8] N. do Trad. Ver §289.

segunda classe. Pois, se yy fosse um quadrado do referido tipo, então surgiria de repente três novas classes de não-resíduos e o número de não-resíduos seria = $6n$ e, se os não-resíduos estiverem agora completados, teríamos que $7n = 4q$.

434. De fato, mostra-se da seguinte forma que não há tal quadrado, arrastando com si três novas classes de não-resíduos: Haveria três classes que surgiriam de tal quadrado e que deveriam ser acrescidas às outras[9]:

IV. y, αy, βy, γy, *etc*.

V. y^2, αy^2, βy^2, γy^2, *etc*.

VI. y^3, αy^3, βy^3, γy^3, *etc*.,

cada uma das quais conteria n termos; deve-se considerar dois casos, um em que xy seja resíduo, o outro em que seja não-resíduo.

435. Seja xy um resíduo. Então, todos os termos da quarta classe, multiplicados por x, isto é, xy, αxy, βxy, γxy, *etc*., sendo n em quantidade, serão resíduos. Mas, também todos os termos da terceira classe, multiplicados por x, a saber, x^4, αx^4, βx^4, γx^4, *etc*., serão o mesmo número de resíduos, mas distintos daqueles; pois, se αxy e βx^4 fossem equivalentes, $\alpha y - \beta x^3$ seria divisível pelo divisor e αy cairia na terceira classe , contra a

[9] N. do Trad. Isto é, às classes listadas em §426.

hipótese. Haveria, portanto, 2*n* resíduos distintos, que é absurdo e, assim, não é possível que *xy* seja um resíduo.

436. Sendo eliminado, portanto, o caso em que *xy* fosse um resíduo, suponhamos que *xy* seja um não-resíduo e, visto que todos os não-resíduos são compreendidos em seis classes, *xy* deve ocorrer em uma delas; mas, se pomos *xy* equivalente a αx, ou αx^2, ou αx^3, ou αy, ou αy^2, ou αy^3, haverá um absurdo[10], pois ou *y* seria um resíduo, ou cairia ou na classe I ou na classe II de não-resíduos, ou *x* seria um resíduo, ou cairia ou na classe IV ou na classe V.

437. Visto que não é possível admitir seis classes de não-resíduos, as mesmas são compreendidas por apenas três classes, que é o resultado procurado, ou por mais do que seis. Caso o último acontecer, todos os quadrados não-resíduos não ocorrerão nas classes II e V. Seja, portanto, *zz* um quadrado não contido nessas duas classes; surgirão, a partir dele, três novas classes, contendo, cada uma, *n* termos:

VII. z, αz, βz, *etc*.

VIII. z^2, αz^2, βz^2, *etc*.

IX. z^3, αz^3, βz^3, *etc*.

438. Ora, como foi mostrado em §435, nem *xy*, nem *xz*, nem *yz* pode ser um resíduo, pois então teria mais resíduos do

[10] N. do Trad. Lembramos que, por hipótese, *y* pertence à classe IV e *x* à classe I.

que realmente existem. Mais ainda, se xy fosse contido em qualquer uma das primeiras seis classes, os mesmos inconvenientes que antes seriam ocasionados; desta forma, xy deveria estar em alguma das três classes restantes. Vejamos, então, se xy puder ser equivalente ao próprio αz.

439. Seja, então, xy equivalente a αz e xz, porque certamente é um não-resíduo, seria equivalente[11] a ou βy, ou βy^2, ou βy^3. Assim, visto que $xy-\alpha z$ e $xz-\beta y^\nu$, onde ν denota ou 1 ou 2, ou 3, seriam divisíveis por $4q+1$, teríamos que $z(xy-\alpha z)-y(xz-\beta y^\nu)$, isto é, $\beta y^{\nu+1}-\alpha z^2$, também seria divisível e, assim, αz^2 seria equivalente a $\beta y^{\nu+1}$ e, portanto seria contido em alguma outra classe, o que é absurdo.

440. Assim, é demonstrado[12] que, se o divisor primo for $4q+1$, a quantidade de resíduos distintos dos biquadrados será = q, nem mais, nem menos, e os não-resíduos serão compreendidos em três classes, em cada uma das quais há q termos.

441. Por isto, visto que os resíduos distintos surgem dos biquadrados $1, 2^4, 3^4, 4^4, ..., 16q^4$, cuja quantidade é = $2q$, devem ser iguais de dois em dois. Assim, se a for um número qualquer menor que $2q$, sempre haverá um, e somente um, outro b,

[11] N. do Trad. Compare isto com §436.
[12] N. do Trad. De fato, a demonstração é incompleta.

igualmente não maior que $2q$, tal que b^4 e a^4 deixem resíduos iguais, ou seja, tal que b^4-a^4 seja divisível por $4q+1$.

442. Ainda mais, visto que tanto $b-a$ quanto $b+a$ são menores que $4q+1$, teremos que $aa+bb$ é divisível por $4q+1$. Em consequência, dado um número primo $4q+1$, sempre pode ser exibida uma soma de dois quadrados $aa+bb$ por ele divisível, de tal forma que nenhuma das duas raízes supera $2q$ e uma ou outra pode ser tomado à vontade.

443. Já mostramos acima[13] que a soma de dois quadrados, primos entre si, $aa+bb$, não admite divisores primos além de dois, a não ser que tenham a forma $4q+1$. Disto se vê que pode ser concluído que todos os números primos da forma $4q+1$ são somas de dois quadrados, bem como que, com certeza, $2(4q+1)$, $5(4q+1)$, $13(4q+1)$, *etc*. também serão a soma de dois quadrados.

444. Embora já foi completamente demonstrado que não há mais do que dois biquadrados, cujas raízes não excedem $2q$ e que deixam o mesmo resíduo, isto[14] também pode ser demonstrado separadamente. Suponha, então, que a, b e c sejam três números que não excedem $2q$, tais que tanto $aa+bb$, quanto

[13] N. do Trad. Em §316.

[14] N. do Trad. Sob as dadas condições, o fato de, para um dado a tem um único b, tal que a^2+b^2 é divisível por $4q+1$, é uma consequência das propriedades (em §440 e §441) dos resíduos dos biquadráticos. Agora, Euler mostra (por redução ao absurdo) essa unicidade sem recorrer às referidas propriedades.

$aa+cc$ e $bb+cc$ são divisíveis por $4q+1$; assim, as diferenças $aa-cc$, $aa-bb$ e $bb-cc$ seriam divisíveis. No entanto, visto que nem $a-c$, nem $a+c$ podem ser divididos por $4q+1$, seu produto $aa-cc$ certamente não pode ser dividido.

445. Temos demonstrado, portanto, por um outro raciocínio, que, se o divisor primo for $4q+1$, a quantidade de resíduos distintos surgidos de biquadrados é $= q$ e não pode haver menos; em consequência, a quantidade de não-resíduos será $3q$, separados nas três classes mencionadas acima.

446. Assim, os resíduos dos biquadrados surgidos do divisor primo $4q+1$, que são 1, α, β, γ, δ, *etc*., têm a seguinte propriedade: α^q-1, β^q-1, γ^q-1, *etc*. admite[15] divisão pelo referido número primo $4q+1$. Deveria ser investigado se, ou não, todos os resíduos têm essa propriedade.

447. Seja xx um não-resíduo; assim, ambos x e x^3 serão não-resíduos. Ora, se $(xx)^q-1$, ou seja, $x^{2q}-1$, fosse divisível por $4q-1$, todos os termos αx^2, βx^2, γx^2, *etc*. gozariam da mesma propriedade; desta forma, visto que os próprios resíduos gozam dessa propriedade, todos os quadrados de 1 até $4qq$ seriam munidos da mesma.

[15] N. do Trad. Ver §421. Na próxima sentença Euler pergunta se a referida propriedade dos resíduos dos biquadrados pode, ou não, ser estendida aos resíduos dos quadrados.

448. Essa propriedade pertenceria, portanto, a todos os números de 1 até $2q$, de tal modo que suas potências de expoente $2q$, quando divididas por $4q+1$, deixariam a unidade; mas, assim, todas as diferenças entre dois termos da série 1, 2^{2q}, 3^{2q}, 4^{2q}, ..., $(2q)^{2q}$ seriam divisíveis por $4q+1$. Que isto é absurdo, porém, já foi visto[16] acima.

449. Desta maneira, faz-se o que foi proposto, a saber, se o quadrado xx for um não-resíduo, então $x^{2q}-1$ certamente não será divisível por $4q+1$. Visto que x e x^3 também são não-resíduos, nem tampouco serão as fórmulas x^q-1, ou $x^{3q}-1$, divisíveis por $4q+1$; disto, é claro que, se a^q-1 admitir divisão por $4q+1$, então o número a será necessariamente achado entre os resíduos dos biquadrados.

450. Logo, quando a potência a^q, dividida por um número primo $4q+1$, deixar a unidade, então todos os resíduos que surgem a partir da série de potências, 1, a, a^2, a^3, a^4, *etc*., serão contidos entre nossos resíduos de biquadrados. E, ao contrário, se a não for um resíduo dos biquadrados, a fórmula a^q-1 certamente não será divisível por $4q+1$.

451. Se q for um número ímpar, -1, ou seja $4q$, não ocorrerá entre os resíduos, pois $(-1)^q-1$ certamente não pode ser dividido por $4q+1$. Nesse caso, portanto, se os resíduos forem 1,

[16] N. do Trad. Ver a nota de Euler (*) após §392.

α, β, γ, δ, *etc*., seus simétricos -1, $-\alpha$, $-\beta$, $-\gamma$, *etc*., ou seja, $4q$, $4q+1-\alpha$, $4q+1-\beta$, $4q+1-\gamma$, *etc*., com certeza serão achados entre os não-resíduos.

452. Segue disto que, se q for um número ímpar, não haverá dois biquadrados a^4 e b^4, cuja soma a^4+b^4 fosse divisível pelo número $4q+1$. Pois, se o resíduo de a^4 fosse α, o de b^4 seria $-\alpha$, o que acabamos de mostrar não pode ser feito.

453. Ao contrário, porém, se q for um número par, certamente -1 ocorrerá entre os resíduos dos biquadrados, pois, se fosse um não-resíduo, $(-1)^q-1$ não seria divisível por $4q+1$. Visto que é divisível, porém, a proposição é claro; isto é, os simétricos de cada resíduo, ou seja, seus complementos, são contidos entre os resíduos dos biquadrados.

454. Se, portanto, q for um número par e $4q+1$ for um número primo, isto é, se $8q+1$ for um número primo, dado um biquadrado qualquer a^4, haverá um outro b^4, tal que sua soma a^4+b^4 seja divisível por $8q+1$. Assim, dado um número a, um número x sempre pode ser achado para o qual a soma dos biquadrados a^4+x^4 seja divisível por 17, ou 41, ou 73, ou 89, ou 97, *etc*.

455. Ao contrário, não há soma alguma de dois biquadrados que seja divisível por qualquer número primo da série 5, 13, 29, 37, 53, 61, 101, *etc*., nem tampouco por qualquer

número primo da forma $4q-1$, pois nem a soma de dois quadrados[17] é divisível por um número de tal forma.

456. Assim, a soma de dois biquadrados, primos entre si, não pode ter outros divisores, além de dois, a não ser os que são compreendidos pela forma $8q+1$, tais como[18]:

$1+2^4 = 17$	$2^4+3^4 = 97$	$4^4+5^4 = 881$	$7^4+8^4 = 73\cdot89$
$1+3^4 = 2\cdot41$	$2^4+5^4 = 641$	$4^4+7^4 = 2657$	$7^4+9^4 = 2\cdot4481$
$1+4^4 = 257$	$2^4+7^4 = 2417$	$4^4+9^4 = 17\cdot401$	$7^4+10^4 = 12401$
$1+5^4 = 2\cdot313$	$2^4+9^4 = 6577$	$5^4+6^4 = 17\cdot113$	$8^4+9^4 = 10657$
$1+6^4 = 1297$	$3^4+4^4 = 337$	$5^4+7^4 = 2\cdot17\cdot89$	$9^4+10^4 = 16561.$
$1+7^4 = 2\cdot1201$	$3^4+5^4 = 2\cdot353$	$5^4+8^4 = 4721$	
$1+8^4 = 17\cdot241$	$3^4+7^4 = 2\cdot17\cdot73$	$5^4+9^4 = 2\cdot3593$	
$1+9^4 = 2\cdot17\cdot193$	$3^4+8^4 = 4177$	$6^4+7^4 = 3697$	
$1+10^4 = 73\cdot137$	$3^4+10^4 = 17\cdot593$		

457. Procura-se agora os divisores, para os quais 2 é achado entre os resíduos, o que não aconteceu nos casos calculados em §424. Mas, de fato, onde 2 ocorrer, também ocorrerá 2α; portanto, o divisor $4q+1$ deve ser um fator dos números a^4-2b^4, ou seja, $2b^4-a^4$. Assim, os seguintes divisores serão incluídos:

73, 89, 113, 233, 281, 353, 593, 617, 937, 1249, 1889, 2273,

2393, 4177,4721, 4801, 6529, *etc*.

Vê-se que esses números são contidos na forma $64pp+qq$. (*)

[17] N. do Trad. Ver §417 ou §279. Os primos até 101, não mencionados nesse parágrafo ou no parágrafo anterior, são da forma $4q-1$.

[18] N. do Trad. No original, há, na última linha da segunda coluna, $2\cdot17\cdot593$ e, na última linha da quarta coluna, 16511.

(*). Escrito na margem. Para 3 ser um resíduo, o divisor deve ser $pp+qq$, de tal modo que ou $p = 12m$, ou $p = 3(2m+1)$ e $q = 4n+2$. Para 5 ser resíduo, o divisor é feito $= 100pp+qq$.

458. Ainda mais, números contidos na fórmula $64pp+qq$ são:

73, 89, 113, 233, 257, 281, 337, 353, 577, 593, 601, 617, 881, 937, 1033, 1049, 1097, 1153, 1193, 1201, 1249, *etc*.

Visto que todos os precedentes ocorrem aqui e o restante seria satisfeito por inspeção, nada há o que nos levaria a duvidar a verdade da conjectura e, como todos esses números são da forma $8n+1$, tanto -2, quanto 2, serão achados entre os resíduos.

459. Examinado todos os divisores primos da forma $4q+1$ até 101, o número q sempre ocorre entre os resíduos e, desta forma q^q-1 seria divisível por $4q+1$; na medida em que isto seja verdadeiro em geral, todos os números q, q^2, q^3, $16q$, $81q$, $256q$, $16qq$, $81qq$, e, portanto, -4, $q-20$, -64, $-4q$ estarão entre os resíduos.

460. Essa observação é corroborada[19] por §339, onde observamos que o número 2 estará entre os resíduos dos quadrados se o divisor primo for da forma $8p+1$, mas será um

[19] N. do Trad. No texto original, há §389. O conteúdo da referido parágrafo, porém, não corresponde à afirmação que Euler faz aqui.

não-resíduo se o divisor for da forma $8p+5$, pois $2^{4p}-1$ é divisível por $8p+1$, enquanto $2^{4p+2}-1$ não é divisível por $8p+5$, mas, visto que $2^{8p+4}-1$ é divisível, é necessário que $2^{4p+2}+1$ seja divisível por $8p+5$.

461. Visto que a forma $4q+1$ se torna $8p+1$ quando q é um número par, neste caso, $2^{2q}-1$, ou seja, 4^q-1, é divisível por $4q+1$ e, portanto, o número 4, bem como seu simétrico -4, devem ser achados entre os resíduos dos biquadrados. Mas, se q for um número ímpar, em qual caso $4q+1$ se torna $8p+5$, teremos que $2^{2q}+1$, ou seja, 4^q+1, ou ainda $(-4)^q-1$, será divisível por $4q+1$; assim, nesse caso, -4 também deve ser achado entre os resíduos dos biquadrados.

462. Para o divisor primo $4q+1$, portanto, seja q um número par, seja ímpar, -4 sempre será achado entre os resíduos dos biquadrados e, em consequência, visto que 1 é também representado por $-4q$, também q deve estar nos mesmos; assim, a primeira[20] observação é corroborada pela segunda.

[20] N. do Trad. Isto é, a observação de q ser um resíduo. Ver §459.

Capítulo XIII

Sobre resíduos surgidos da divisão de surdosólidos[1] por números primos

463. Se o divisor for d e a^5 deixar α, então $(d–a)^5$ deixará $–\alpha$ e, desta maneira, todos os resíduos nascerão a partir das potências 1^5, 2^5, 3^5, 4^5, ..., $(d–1)^5$; se estes foram todos distintos, sua quantidade será = $d–1$.

464. Sejam 1, α, β, γ, *etc*. todos os resíduos distintos, então os produtos dois a dois ocorrerão entre os mesmos; mais ainda, se o produto mn, bem como um dos fatores m, pertencerem ali, o outro fator n também ali pertencerá. Pois, se mn surgir de a^5 e m de b^5, então mn também surgirá de nb^5 e teremos que $a^5–nb^5$ é divisível por d. Mas, pode-se fazer $a = fb \pm gd$ e, portanto, a^5 deixa o mesmo resíduo que f^5b^5; assim, visto que $f^5b^5–nb^5$ e, portanto $f^5–n$, é divisível por d, o número n estará nos resíduos.

465. Se a estiver nos resíduos, então a^2, a^3, a^4, a^5 também estarão no mesmo lugar (mas, esse último estará ali em qualquer caso). Por sua vez, se a^2 estiver nos resíduos, $a^3 = a^5:a^2$

[1] N. do Trad. Isto é, quintas potências. Ver a Introdução.

também estará no mesmo lugar[2], e, porque a^4 é resíduo, a também será um resíduo. Logo, se qualquer potência a^n (a menos que n fosse um múltiplo de cinco) for um resíduo, todas suas potências a, a^2, a^3, *etc*. serão simultaneamente resíduos.

466. Seja m a quantidade de resíduos 1, α, β, γ, δ, *etc*. para o divisor primo $2q+1$; se todos os números menores que o divisor ocorrerem entre os resíduos, teremos que $m = 2q$. Será claro, em breve,[3] que há tais casos.

467. Se tivermos que $m < 2q$, haverá um não-resíduo, digamos A, e, portanto, em primeiro lugar, haverá m não-resíduos, A, $A\alpha$, $A\beta$, *etc*.; mas, também, visto que A^2, A^3 e A^4 são não-resíduos, a partir de cada um, mais m novos são obtidos, de tal forma que um único não-resíduo A acarreta quatro classes de não-resíduos

I. A, $A\alpha$, $A\beta$, $A\gamma$, *etc*.
II. A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, *etc*.
III. A^3, $A^3\alpha$, $A^3\beta$, $A^3\gamma$, *etc*.
IV. A^4, $A^4\alpha$, $A^4\beta$, $A^4\gamma$, *etc*.

468. Sempre que tivermos um não-resíduo, portanto, haveremos de imediato $4m$ não-resíduos e, se estes forem todos, será necessário que $m+4m = 2q$, ou seja, $5m = 2q$ e $m = \frac{2q}{5}$ e, portanto, não poderia haver não-resíduo algum, a menos que q fosse um múltiplo de cinco.

[2] N. do Trad. Visto que a^2 é resíduo por hipótese e o produto $a^2a^3 = a^5$ é resíduo, a^3 é resíduo por §464.
[3] N. do Trad. Ver §468.

469. Mas, se tiver um novo não-resíduo B, além das quatro classes, dele surgirão as seguintes quatro classes:

V. B, $B\alpha$, $B\beta$, $B\gamma$, *etc*. VII. B^3, $B^3\alpha$, $B^3\beta$, $B^3\gamma$, *etc*.

IV. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, *etc*. VIII. B^4, $B^4\alpha$, $B^4\beta$, $B^4\gamma$, *etc*.

No entanto, uma contradição[4] segue, seja AB considerado um resíduo, seja um não-resíduo; em consequência, é necessário que todos os não-resíduos que existem sejam exauridos pelas quatro classes anteriores.

470. Com certeza, então, sempre que o número q do divisor primo $2q+1$ não for um múltiplo de cinco, todos os números ocorrerão entre os resíduos e a sua quantidade será = $2q$. E, portanto, não haverá dois números a e b, menores que $2q+1$, tais que a^5-b^5 seja divisível por $2q+1$; e, assim, também $a^4+a^3b+aabb+ab^3+b^4$ não pode ser dividido por qualquer número primo $2q+1$, em que q não fosse um múltiplo de cinco.

471. Desta forma, todos os divisores primos de números da forma $a^4+a^3b+aabb+ab^3+b^4$, ou mesmo de a^5-b^5, excluindo o divisor $a-b$, são contidos na forma $10p+1$ e os referidos números não podem ser divididos, de forma alguma, por qualquer número contido nas fórmulas $10p+3$, $10p+7$ e $10p+9$.

[4] N. do Trad. Presumivelmente, o argumento de Euler seria algo assim: Seja AB um resíduo, digamos α. Agora, ao multiplicar os elementos de classe IV por A, obtemos m resíduos distintos; portanto um deles, digamos $A(A^4\beta)$, é (equivalente a) α. Assim, $d \mid AB-A(A^4\beta)$ e, portanto, $d \mid B-A^4\beta$, o que implica que B pertence à classe IV, contra a hipótese. Por outro lado, se AB for um não-resíduo, pertencerá a uma das oito classes de não-resíduos. Mas, semelhante aos argumentos análogos nos capítulos anteriores, cada uma das possibilidades nos leva a uma contradição.

472. Mas, se o divisor primo for $10p+1$, nem todos os números ocorrerão na classe dos resíduos, pois, se todos ocorressem, $x^{2p}-1$ sempre seria divisível por $10p+1$, qualquer que seja x, isto é, as diferenças de todas as potências $1, 2^{2p}, 3^{2p}, 4^{2p}, \ldots, (2p+1)^{2p}$ seriam divisíveis por $10p+1$, cuja absurdidade foi mostrado acima[5].

473. Por essa razão, se o divisor primo for $10p+1$, a quantidade de resíduos distintos será apenas $= 2p$ e haverá $8p$ não-resíduos; em consequência, sempre haverá números, de cinco em cinco, a, b, c, d, e, menores que $10p+1$, cujas quintas potências produzem resíduos iguais.

474. Seja proposto, por exemplo, um número a qualquer; sempre pode-se determinar quatro outros, b, c, d, e, cada um menor que o divisor $10p+1$, tais que os seguintes números são por ele divisível:

os números	e, portanto, esses também
b^5-a^5	$b^4+ab^3+a^2b^2+a^3b+a^4$
c^5-a^5	$c^4+ac^3+a^2c^2+a^3c+a^4$
d^5-a^5	$d^4+ad^3+a^2d^2+a^3d+a^4$
e^5-a^5	$e^4+ae^3+a^2e^2+a^3e+a^4$.

A demonstração disto é uma modificação da mesma para as potências precedentes.

[5] N. do Trad. Ver a nota de Euler (*) após §392.

475. Assim, também as primeiras destes, diminuídas pelas três seguintes, podem ser divididas pelo mesmo divisor; mais ainda, essas diferenças[6], quando divididas por $b–c$, $b–d$, e $b–e$, pois são pelos mesmos divisíveis, resultam nas seguintes:

$$b^3+b^2c+bc^2+c^3+ab^2+abc+ac^2+a^2b+a^2c+a^3,$$
$$b^3+b^2d+bd^2+d^3+ab^2+abd+ad^2+a^2b+a^2d+a^3,$$
$$b^3+b^2e+be^2+e^3+ab^2+abe+ae^2+a^2b+a^2e+a^3.$$

476. Novamente, as diferenças destes, divididas, por sua vez, por $c–d$ e $c–e$ ainda devem ser divisíveis por $10p+1$; os resultados são:

$$c^2+cd+d^2+bc+bd+b^2+ac+ad+ab+a^2,$$
$$c^2+ce+e^2+bc+be+b^2+ac+ae+ab+a^2,$$

e, de novo, a diferença desses, divididas por $d–e$, resulta em:

$$e+d+c+b+a$$

477. Desta forma, é claro que os cinco números, a, b, c, d, e, cujas quintas potências, quando divididas por $10p+1$, deixam resíduos iguais, são constituídos de tal forma que a sua soma

$$a+b+c+d+e$$

é divisível pelo referido divisor. Mais ainda, visto que cada um deles é menor que $10p+1$, sua soma é ou $10p+1$, ou $2(10p+1)$, ou $3(10p+1)$, ou $4(10p+1)$.

[6] N. do Trad. Isto é, $b^4+ab^3+a^2b^2+a^3b+a^4–(c^4+ac^3+a^2c^2+a^3c+a^4)$, quando dividido por $c^4+ac^3+a^2c^2+a^3c+a^4$ resulta em $b^3+b^2c+bc^2+c^3+ab^2+abc+ac^2+a^2b+a^2c+a^3$, *etc*.

478. Como é permitido considerar números negativos como resíduos, a referida soma pode ser pensada igual a zero[7]; disto, o quinto é dado em termos dos outros quatro, a, b, c, d, isto é, $e = -a-b-c-d$, e, visto que isto é único, é claro que não há mais do que cinco.

479. Eis, então, uma nova demonstração de que a quantidade de resíduos diversos para qualquer divisor primo $2q+1$ seja ou $= 2q$, ou $= \frac{2q}{5}$, e que o primeiro sempre acontece quando q não é um múltiplo de cinco, o segundo, sempre que $q = 5p$. No primeiro caso, todos os números menores que o divisor são resíduos; no segundo, apenas uma quinta parte deles são resíduos.

480. Dado, portanto, um divisor primo $10p+1$, a quantidade de resíduos distintos é $= 2p$, entre os quais números negativos ocorrem; disto, a quantidade deles é par. Assim, o mesmo resíduo é equivalente a cinco potências distintas cujas raízes são menores que o divisor, e será útil listá-las.

481. Visto que tais divisores são 11, 31, 41, 61, 71, 101, *etc*., consideremos, em primeiro lugar, o divisor $10p+1 = 11$, o que faz $p = 1$:

[7] N. do Trad. Ver §463. Isto é evidente na linguagem de congruências, pois se $d \mid n$, então $n \equiv 0 \pmod{d}$.

Resíduos	das potências	Classes de não-resíduos			
		I.	II.	III.	IV.
1	$1^5,\ 3^5,\ 4^5,\ 5^5,\ 9^5$	2	4	8	5
10	$2^5,\ 6^5,\ 7^5,\ 8^5,\ 10^5$	9	7	3	6.

482.Se o divisor for $10p+1 = 31$ e $p = 3$, teremos:

Resíduos	das potências	Classes de não-resíduos			
		I.	II.	III.	IV.
1	$1^5,\ 2^5,\ 4^5,\ 8^5, 16^5$	2	4	8	16
5	$7^5, 14^5, 19^5, 25^5, 28^5$	10	20	9	18
26	$3^5,\ 6^5, 12^5, 17^5, 24^5$	21	11	22	13
6	$11^5, 13^5, 21^5, 22^5, 26^5$	12	24	17	3
25	$5^5,\ 9^5, 10^5, 18^5, 20^5$	19	7	14	28
30	$15^5, 23^5, 27^5, 29^5, 30^5$	29	27	23	15

483. Se o divisor primo for $10p+1 = 41$ e, portanto, $p = 4$, teremos:

Resíduos	das potências	Classes de não-resíduos			
		I.	II.	III.	IV.
1	$1^5, 10^5, 16^5, 18^5, 37^5$	2	4	8	16
40	$4^5, 23^5, 25^5, 31^5, 40^5$	39	37	33	25
3	$11^5, 12^5, 28^5, 34^5, 38^5$	6	12	24	7
38	$3^5,\ 7^5, 13^5, 29^5, 30^5$	35	29	17	34
9	$5^5,\ 8^5,\ 9^5, 21^5, 39^5$	18	36	31	21
32	$2^5, 20^5, 32^5, 33^5, 36^5$	23	5	10	20
14	$15^5, 22^5, 24^5, 27^5, 35^5$	28	15	30	19
27	$6^5, 14^5, 17^5, 19^5, 26^5$	13	26	11	22

484. Se o divisor primo for $10p+1 = 61$ e $p = 6$, teremos:

Resíduos	das potências	Classes de não-resíduos I.	II.	III.	IV.
1	1^5, 9^5, 20^5, 34^5, 58^5	2	4	8	16
60	3^5, 27^5, 41^5, 52^5, 60^5	59	57	53	45
13	12^5, 25^5, 42^5, 47^5, 57^5	26	52	43	25
48	4^5, 14^5, 19^5, 36^5, 49^5	35	9	18	36
14	5^5, 39^5, 45^5, 46^5, 48^5	28	56	51	41
47	13^5, 15^5, 16^5, 22^5, 56^5	33	5	10	20
11	8^5, 11^5, 28^5, 37^5, 38^5	22	44	27	54
50	23^5, 24^5, 33^5, 50^5, 53^5	39	17	34	7
21	10^5, 17^5, 29^5, 31^5, 35^5	42	23	46	31
40	26^5, 30^5, 32^5, 44^5, 51^5	19	38	15	30
29	6^5, 21^5, 43^5, 54^5, 59^5	58	55	49	37
32	2^5, 7^5, 18^5, 40^5, 55^5	3	6	12	24

485. Sendo proposto, portanto, qualquer divisor primo da forma $10p+1$, há um número a, tal que a^5-1 é por ele divisível; também os números a^2, a^3, a^4 haverá a propriedade de que suas quintas potências deixam a unidade[8]. Os termos seguintes, a^5, a^6, *etc*., não são distintos destes, pois, visto que $a^5 = n(10p+1)+1$, a^5 é equivalente a 1, a^6 a a, a^7 a a^2, *etc*.

[8] N. do Trad. Usando congruências, temos $(a^2)^5 = (a^5)^2 \equiv 1^2 \equiv 1$. Presumivelmente, porém, Euler teria usado fatoração. Por exemplo, $d \mid a^5-1 \Rightarrow d \mid (a^3)^5-1 = (a^5-1)(a^{10}+a^5+1)$.

486. Visto que há cinco números cujas quintas potências, divididas por $10p+1$, deixam a unidade, eles podem ser representados assim: 1, a, a^2, a^3, a^4 e, se b^5 deixa o resíduo α, teremos cinco números, b, ab, a^2b, a^3b, a^4b, cujas quintas potências, quando divididas por $10p+1$, deixam o mesmo resíduo α.

487. Porque o mesmo pode se estender para potências maiores, sendo proposto qualquer número primo $mn+1$, sempre haverá um número a, tal que a^m-1 é por ele divisível; todas as suas potências serão fornecidas com a mesma propriedade. Mais ainda, para a menor que o divisor $mn+1$, pode-se exibir tantos números distintos desse tipo quanto m tem de unidades.

488. Assim, seja proposto o divisor primo $mn+1$. Se potências 1^m, 2^m, 3^m, 4^m, *etc*., até $(mn)^m$, forem por ele divididas, não deixarão mais que n resíduos diversos e, portanto, haverá $(m-1)n$ números distintos, menores que o divisor, que não são resíduos.

489. Seja a o menor número depois da unidade, cuja potência a^m, dividida por $mn+1$ deixa a unidade. Sempre haverá um número deste tipo e, de fato, será único. Então, se a potência b^m deixar α, as potências com expoente m de todos os números b, ab, a^2b, a^3b, ..., $a^{m-1}b$, cuja quantidade é = m, deixarão o mesmo resíduo α.

490. Seja $m = 2$; então as menores potências a^2 que, quando divididas pelo número primo $2n+1$, deixam a unidade, são como segue

$2n+1$	n	a^2
3	1	2^2
5	2	4^2
7	3	6^2
11	5	10^2

e assim por diante. Neste caso, sempre temos $a = 2n$.

491. Seja $m = 3$; então as potências a^3 que, divididas por $3n+1$, deixam a unidade são

$3n+1$	n	potências	$3n+1$	n	potências
7	2	$1^3, 2^3, 4^3$	61	20	$1^3, 13^3, 47^3$
13	4	$1^3, 3^3, 9^3$	67	22	$1^3, 29^3, 37^3$
19	6	$1^3, 7^3, 11^3$	73	24	$1^3, 8^3, 64^3$
31	10	$1^3, 5^3, 25^3$	79	26	$1^3, 23^3, 55^3$
37	12	$1^3, 10^3, 26^3$	97	32	$1^3, 35^3, 61^3$
43	14	$1^3, 6^3, 36^3$	103	34	$1^3, 46^3, 56^3$.

492. Seja $m = 4$; então as potências a^4 que, divididas por $4n+1$, deixam a unidade são

$4n+1$	n	potências	$4n+1$	n	potências
5	1	$1^4, 2^4, 4^4, 3^4$	53	13	$1^4, 23^4, 52^4, 30^4$
13	3	$1^4, 5^4, 12^4, 8^4$	61	15	$1^4, 11^4, 60^4, 50^4$
17	4	$1^4, 4^4, 16^4, 13^4$	73	18	$1^4, 27^4, 72^4, 46^4$
29	7	$1^4, 12^4, 28^4, 17^4$	89	22	$1^4, 34^4, 88^4, 55^4$
37	9	$1^4, 6^4, 36^4, 31^4$	97	24	$1^4, 22^4, 96^4, 75^4$
41	10	$1^4, 9^4, 40^4, 32^4$	101	25	$1^4, 10^4, 100^4, 91^4$.

493. Seja $m = 5$; então as potências a^5 que, divididas por $5n+1$, deixam a unidade sào, como já vimos[9],

$5n+1$	n	potências
11	2	1^5, 3^5, 9^5, 5^5, 4^5
31	6	1^5, 2^5, 4^5, 8^5, 16^5
41	8	1^5, 10^5, 18^5, 16^5, 37^5
61	12	1^5, 9^5, 20^5, 58^5, 34^5
71	14	1^5, 5^5, 25^5, 54^5, 57^5
101	20	1^5, 36^5, 84^5, 95^5, 87^5.

494. Seja $m = 6$; então as seis potências a^6 que, divididas por $6n+1$, deixam a unidade são

$6n+1$	n	potências
7	1	1^6, 2^6, 4^6, 6^6, 5^6, 3^6
13	2	1^6, 3^6, 9^6, 12^6, 10^6, 4^6
19	3	1^6, 7^6, 11^6, 18^6, 12^6, 8^6

aqui, claro, as mesmas potências são produzidas como no caso de $m = 3$, juntado o mesmo tanto que surge de raízes negativas[10].

495. Seja $m = 7$; então as potências a^7 que, divididas por $7n+1$, deixam a unidade são

$7n+1$	n	potências
29	4	1^7, 7^7, 20^7, 24^7, 23^7, 16^7, 25^7
43	6	1^7, 4^7, 16^7, 21^7, 41^7, 35^7, 11^7
71	10	1^7, 20^7, 45^7, 48^7, 37^7, 30^7, 32^7
113	16	1^7, 16^7, 30^7, 28^7, 109^7, 49^7, 106^7.

[9] N. do Trad. Os casos $n = 2, 6, 8$ e 12 são apresentados em §§481-484; observe que $n = 2p$.

[10] N. do Trad. Isto é, $d \mid a^3-1 \Rightarrow d \mid a^6-1 = (a^3-1)(a^3+1)$ e $d \mid a^6-1 \Rightarrow d \mid (-a)^6-1$.

496. Já observamos[11] que, sendo conhecido um destes números, o restante surgem das potências deste. De fato, um método[12] bastante rápido para achar tal número seria o seguinte. Proposto um divisor primo $mn+1$, procura-se duas potências a^m e b^m que fornecem o mesmo resíduo; então, procura-se x, tal que $x = \frac{b + p(mn+1)}{a}$, e x^m deixará a unidade. Mais ainda, p sempre pode ser tomado de tal forma a fazer x um inteiro.

497. Sendo $mn+1$ o divisor primo, sejam as potências de expoente m, que deixam a unidade, as seguintes:

$$1^m, \alpha^m, \beta^m, \gamma^m, \delta^m, \textit{etc}.,$$ em quantidade de m.

Então, 1, α, β, γ, δ, *etc*. serão os resíduos que surgem da progressão geométrica 1, α, α^2, α^3, α^4, *etc*; serão também, portanto, os que surgem da série de potências 1^n, 2^n, 3^n, 4^n, 5^n, 6^n, *etc*.

498. Eis, então, um método facílimo para achar pelo menos um número α, tal que $\alpha^m - 1$ seja divisível por $mn+1$; claramente, sempre pode-se tomar 2^n para α, ou seja, o resíduo que surge dessa potência de dois, e os valores apropriados

[11] N. do Trad. Em §485, Euler observa isto para o caso n = 5 e, em §486, faz uma generalização para resíduos diferentes da unidade.

[12] N. do Trad. Em termos modernos, o método consiste em achar três termos a, b e x, tais que, módulo d, $a^m \equiv b^m \equiv \alpha$ e $\alpha x^m \equiv \alpha$; então α, visto que é coprimo com o número primo d, pode ser cancelado.

podem ser procurados a partir de 3^n, 5^n, *etc*. Sendo um conhecido, o restante é facilmente achado.

499. Se, para o divisor primo $mn+1$, o número N ocorrer entre os resíduos das potências 1, 2^n, 3^n, 4^n, *etc*., o número Na^n também ali ocorrerá; e haverá um número x, tal que $x^n - Na^n$ é divisível por $mn+1$, e também $N^m - 1$ será divisível[13] por $mn+1$.

500. Por sua vez, se $N^m - 1$ for divisível por $mn+1$, N será o resíduo de alguma potência x^n; pois, se fosse um não-resíduo, todos os não-resíduos restantes e, portanto, todos os números, teriam a mesma propriedade; mas, então, todos os números $4^m - 1$, $2^m - 1$, $3^m - 1$, *etc*. seriam divisíveis por $mn+1$, o que, porém, não pode ser feito.

501. Dado o divisor primo $mn+1$, sejam 1, A, B, C, D, *etc*. os resíduos das potências 1^m, 2^m, 3^m, 4^m, *etc*. e 1, α, β, γ, δ, *etc*. os resíduos das potências 1^n, 2^n, 3^n, 4^n, *etc*. e, de fato, todas as potências

$$1^m, \alpha^m, \beta^m, \gamma^m, \delta^m, \text{etc}.$$

deixam o resíduo 1; e também as potências 1^n, A^n, B^n, C^n, D^n, *etc*. deixam resíduo 1, portanto, as formas $\alpha^m - A^n$ serão divisíveis por $mn+1$.

[13] N. do Trad. Isto é uma consequência do Teorema de Euler, $a^{\varphi(d)} \equiv 1 \pmod{d}$.

Pagina Intercalada

Tentativa de demonstrar se 2 *é achado entre os resíduos do divisor primo* 8q+7. Supomos que 2 está nos resíduos e, como $(2q+m)^2$ está no mesmo lugar, também $8qq+8mq+2mm$ e, portanto,

$8mq+2mm-7q$ e $2mm-7m-7q$ e $2mm-7m+q+7$,

que, se nunca for um não-resíduo, esclarecerá a proposição. Mas, não-resíduos podem ser representados por quadrados negativos, os dobros dos quais serão resíduos por hipótese; logo, temos

$2mm-7m+q+7 = -2aa+8bq+7b$, e faça

$$q = \frac{2aa+2mm-7m+7-7b}{8b-1} \text{ e } 8q+7 = \frac{(4a)^2+(4m-7)^2}{8b-1},$$

e $8q+7$ seria divisor de $(4a)^2+(4m-7)^2$, mas visto que isto não pode ser feito, segue que nenhum absurdo pode ser deduzido da suposição que 2 é um resíduo. Isto deveria resultar por necessidade, se 2 não fosse resíduo. (*)

(*) *Escrito na margem*. Se $2mm-7m+q+7$ é colocado $= -aa$, faça

$$8q+7 = \frac{2(2a)^2+(4m-7)^2}{8b-1},$$

agora resta a ser demonstrado que $2xx+yy$ nunca é divisível por $8q+7$.

Uma outra nota que parece se relacionado com este. $8xx-(2y+1)^2$ não tem outros divisores primos, exceto os de forma $8n-1$ e $8n+1$

$\frac{8xx-1}{7}$ inteiro se[14] $x = 7a\pm1$, $\frac{8xx-1}{23}$ inteiro se $x =$

$23a\pm7$, $\frac{8xx-1}{31}$ inteiro se $x = 31a\pm2$,

$\frac{8xx-1}{47}$ « $x = 47a\pm10$, $\frac{8xx-1}{17}$ « $x =$

$17a\pm7$, $\frac{8xx-1}{41}$ « $x = 41a\pm6$.

Teorema. Seja o divisor $12q+11$. Então, 3 será um resíduo.

Suponha que 3 é um resíduo e, se nenhum absurdo segue disto, será considerado verdadeiro. Assim, -3 será um não-resíduo e todos os não-resíduos serão $-3aa$. Mas, $(2q+m)^2$ é resíduo, bem como $12qq+12mq+3mm$, e, portanto, $3mm-11q-11m$, e também $3mm+q-11m+11$, que nunca pode ser o não-resíduo $-3aa$: pois ponha

$3mm-11m+11+q = -3aa+12bq+11b$, teremos

[14] N. do Trad. O texto original há apenas "int si", tanto aqui, quanto nos outros dois lugares dessa linha.

$q = \frac{3aa + 3mm - 11m + 11 - 11b}{12b - 1}$, de que obtemos $12q+11 = \frac{(6a)^2 + (6m-11)^2}{12b-1}$,

por isso, visto que é absurdo, $3mm-11m+11+q$ nunca será contido entre os resíduos.

Também para o divisor $8q+7$.

Se 2 fosse um não-resíduo, em geral $2mm-7m-7q\pm\alpha(8q+7)$ seria um não-resíduo, em geral também $(4q+n)^2 = 16qq+8nq+nn = 8nq+nn-14q = nn-14q-7 = nn+2q-7n+14\pm\beta(8q+7)$ seria um resíduo, portanto todos os números seriam contidos em uma ou outra dessas fórmulas:

$$2mm-7m-7q\pm\alpha(8q+7)$$
$$nn-7n-14q\pm\beta(8q+7).$$

Se um único número pode ser achado que não é ali contido, a demonstração será completada; alternativamente, se um mesmo número é contido em ambas as fórmulas, o que é feito pondo $m = f+g$, $n = f+2g$, teríamos $ff-2gg+7g+7q$ divisível por $8q+7$.

Capítulo XIV

Sobre resíduos surgidos da divisão de quadrados por números compostos

502. Sejam 1, α, β, γ, δ, *etc*. os resíduos que surgem da divisão de quadrados pelo número primo $2p+1$, cuja quantidade[1] é $= p$. Vejamos, em primeiro lugar, quais resíduos surgem quando o divisor é dobrado para $2(2p+1)$, excluindo, porém, quadrados pares; pois consideremos apenas os quadrados que são primos com o divisor.

503. A quantidade[2] de quadrados, cujas raízes são menores que o divisor, é $= 2p$ e, porque os quadrados aa e $(4p+2-a)^2$ deixam o mesmo resíduo, a quantidade de resíduos distintos não pode ser maior que p. Logo, será ou $= p$, ou menor que p.

504. Será menor, claro, se houver dois quadrados aa e bb, tais que deixam o mesmo resíduo e não temos $b = 4p+2-a$. Nesse caso, teríamos que $bb-aa = (b-a)(b+a)$ é divisível por $2(2p+1)$ e um fator deve ser divisível por 2, o outro por $2p+1$. Mas, sendo um deles par, o outro também será par e, portanto,

[1] N. do Trad. Ver §289.

[2] N. do Trad. Há $4p+2$ números que não excedem o divisor $d = 4p+2$; deles, $2p+1$ são pares e, portanto, não coprimo com o divisor, como é também o caso do próprio número (primo) $2q+1$. Assim, há $2p$ números menores que o divisor e coprimo a ele.

divisível pelo divisor inteiro; em consequência[3], teríamos $b = 2(2p+1)-a$.

505. A quantidade de resíduos distintos, portanto, que surgem de quadrados pela divisão por primos, será $= p$, o mesmo número que surgem do divisor primo $2p+1$. Sejam 1, A, B, C, D, *etc*. os resíduos surgidos do divisor $2(2p+1)$, cuja quantidade é $= p$; os produtos deles, dois a dois, ocorrerão no mesmo lugar.

506. Mais ainda, há $2p$ números menores que o divisor e primos a ele; assim, como os resíduos constituem apenas metade deles, a outra metade estará na classe de não-resíduos. Sejam eles $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc*., cuja quantidade será $= p$ e os produtos destes, dois a dois, serão novamente resíduos.

507. Examinemos alguns exemplos, tanto dos resíduos surgidos do divisor primo[4] $2p+1$, quanto dos surgidos do seu duplo $2(2p+1)$; ao mesmo tempo, observaremos os não-resíduos primos com o divisor:

divisor	3	6	5	10	7	14
resíduos	1	1	1, 4	1, 9	1, 2, 4	1, 9, 11
não-resíduos	2	5	2, 3	3, 7	3, 5, 6	3, 5, 13

divisor	11	22
resíduos	1, 3, 9, 5, 4	1, 9, 3, 5, 15

[3] N. do Trad. Visto que podemos supor $0 < a < b < 2(2p+1)$, se $2p+1 \mid b-a$, então $b-a = 2p+1$, o que não pode ser, pois, como o próprio Euler observou, $b-a$ tem de ser par.
[4] N. do Trad. Ver §308.

não-resíduos	2, 6, 7, 8, 10	7, 13, 17, 19, 21
divisor	13	26
resíduos	1, 3, 4, 9, 10, 12	1, 3, 9, 17, 23, 25
não-resíduos	2, 5, 6, 7, 8, 11	5, 7, 11, 15, 19, 21
divisor	17	34
resíduos	1, 2,4, 8, 9, 13,15,16	1, 9, 13, 15, 19,21, 25,33
não-resíduos	3, 5, 6, 7,10,11 12,14	3, 5, 7,11, 23, 27, 29, 31

508. Representamos isto de forma geral

divisor	$2p+1$	$2(2p+1)$
resíduos	1, α, β, γ, δ, *etc*.	1, *A*, *B*, *C*, *D*, *etc*.
não-resíduos	$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{e}$, *etc*.	$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, *etc*.

e, em primeiro lugar, observamos que todos os resíduos do divisor $2(2p+1)$, ou eles mesmos, ou diminuído por $2p+1$ constituem os resíduos dos divisores $2p+1$.

509. Claramente, ou *A*, ou $A-(2p+1)$ ocorre entre os resíduos 1, α, β, γ, δ, *etc*. Pois, visto que há um quadrado ímpar *aa*, tal que $aa-A$ é divisível por $2(2p+1)$, será também divisível por $2p+1$; em consequência, é necessário que *A* seja achado entre os resíduos do divisor $2p+1$, ou $A-(2p+1)$, se acontecer que $A > 2p+1$.

510. Ainda mais, os números ímpares da série 1, α, β, γ, δ, *etc*. ocorrem na série 1, *A*, *B*, *C*, *D*, *etc*.; no entanto, os pares não são ali achados, mas, em vez deles, os mesmos aumentados

pelo número $2p+1$. Pois, seja α um número ímpar; visto que $aa-\alpha$ é divisível por $2p+1$, teremos que $aa-\alpha = n(2p+1)$. Ora, a é ou par, ou ímpar. Si for ímpar[5], $aa-\alpha$ será par, assim, n também será par e, portanto, $aa-\alpha$ será divisível por $2(2p+1)$.

511. Mas, se a for par, $2p+1-a$ será ímpar e[6] $(2p+1-a)^2-\alpha = n(2p+1)$, donde n é par, de tal modo que a referida fórmula também será divisível por $2(2p+1)$; em consequência, se α for um número ímpar, será certamente contido entre os resíduos 1, A, B, C, *etc*.

512. Mas, se α for um número par, em vez dele, $\alpha+2p+1$ pode ser considerado entre os resíduos do divisor $2p+1$ e, visto que esse número é ímpar, ele deve ser achado, pelas razões dadas[7], entre os resíduos do divisor $2(2p+1)$.

513. Dados, portanto, os resíduos 1, α, β, γ, δ, *etc*., surgidos do divisor primo $2p+1$, pode-se determinar imediatamente, a partir deles, a série dos resíduos 1, A, B, C, *etc*. surgidos do divisor duplo $2(2p+1)$; para tanto, escolhe-se aqueles entre os mesmos que são ímpares e aumenta-se os pares pelo número $2p+1$.

[5] N. do Trad. Ver §502.
[6] N. do Trad. Ver §284.
[7] N. do Trad. Nos dois parágrafos anteriores.

514. De forma semelhante, da série de não-resíduos 𝔞, 𝔟, 𝔠, 𝔡, *etc*., correspondendo ao divisor 2*p*+1, forma-se a série de não-resíduos, correspondendo ao divisor 2(2*p*+1), tomando os próprios ímpares e aumentando os pares pelo número 2*p*+1.

Sobre o divisor 4(2*p*+1) = *d*.

515. A quantidade[8] de números menores que esse divisor e a ele primos é $2\cdot1\cdot2p = 4p$ e não somente os quadrados *aa* e $(d-a)^2$, mas também dois outros, *bb* e $(d-b)^2$, deixam o mesmo resíduo. Pois, pode-se fazer[9] $bb-aa = (b-a)(b+a) = 4n(2p+1)$, pondo $b-a = 2n$ e $b+a = 2(2p+1)$; em consequência, temos $b = 2(2p+1)-a$ e, desta maneira, quatro quadrados deixarão o mesmo resíduo, sendo suas raízes as seguintes: a, $2(2p+1)-a$, $2(2p+1)+a$, $4(2p+1)-a$.

516. Não pode haver, no entanto, mais que quatro; assim, neste caso o número de resíduos é apenas *p*, como para o divisor primo 2*p*+1. Desta forma, o número de não-resíduos é 3*p*, como pode ser visto dos seguintes exemplos[10]:

[8] N. do Trad. As regas para o cálculo do valor da função φ de Euler são dadas em Capítulo IV.
[9] N. do Trad. Ver §504.
[10] N. do Trad. Ver §308.

divisor	3	12	5	20	7	28
resíduos	1	1	1, 4	1, 9	1, 2, 4	1, 9, 25
não-resíduos	2	5 7 11	2, 3	3, 7 1, 19 3, 17	3, 5, 6	3, 27, 19 5, 17, 13 11, 15, 23

divisor	11	44
resíduos	1, 3, 9, 5, 4	1, 9, 25, 5, 37
não-resíduos	2, 6, 7, 8, 10	3, 27, 31, 15, 23 7, 19, 43, 35, 39 13, 29, 17, 21, 41

divisor	13	52
resíduos	1,3,4,9,10,12	1, 9, 25, 49, 29, 17
não-resíduos	2, 5,6,7, 8,11	3,27, 23, 43, 35, 51 5, 45, 21, 37,41, 33 7, 11,19, 31,47, 15.

517. Sejam 1, α, β, γ, δ, *etc*. os resíduos para o divisor 2*p*+1 e 1, *A*, *B*, *C*, *D*, *etc*. os resíduos, em quantidade igual, para o divisor 4(2*p*+1). Em primeiro lugar, é claro que estes resíduos são achados entre aqueles; especificamente, os da série 1, *A*, *B*, *C*, *D*, *etc*., que são menores que 2*p*+1, são eles mesmos contidos na série 1, α, β, γ, δ, *etc*., enquanto os que são maiores devem ser reduzidos pelo número 2*p*+1, ou seu dobro, ou seu triplo.

518. Em seguida, observo que nenhum número da forma $4q-1$ é contido entre os resíduos 1, A, B, C, D, *etc*. Pois, como o quadrado aa, menos o número $4q-1$, não pode ser dividido[11] por 4, não se pode fazer $aa-(4q-1)$ um múltiplo de $4(2p+1)$; em consequência, os números 3, 7, 11, 15, 19, 23 são sempre entre os não-resíduos.

519. Se um número ímpar da forma $4q+1$ ocorrer na série 1, α, β, γ, δ, *etc*., o mesmo ocorrerá também na série 1, A, B, C, D, *etc*.; pois, se $aa-(4q+1)$ for divisível por $2p+1$, também $(2p+1\pm a)^2-(4q+1)$ será divisível; e, porque, dos números a e $2p+1\pm a$, um é certamente par e o outro ímpar, tomando a ímpar, $aa-(4q+1)$ será divisível por 4 e, portanto, por $4(2p+1)$, de tal forma que, para o referido divisor, $4q+1$ deveria ser um resíduo.

520. Mas, se o número ímpar $4q-1$ for resíduo do divisor $2p+1$, não será resíduo do divisor $4(2p+1)$, como já vimos[12]; mas, então $2(2p+1)+4q-1$, porque se reduz à forma $4r+1$, certamente será contido entre os divisores de $4(2p+1)$.

521. Se o número par $2q$ for resíduo do divisor $2p+1$, então ou

$$2q+2p+1, \quad \text{ou} \quad 2q+3(2p+1)$$

[11] N. do Trad. Observe que $a = 4k\pm1$ ou $a = 4k\pm2$.

[12] N. do Trad. Em §518. Para o resto do presente parágrafo, bem como para o próximo, ver §517.

será resíduo do divisor $4(2p+1)$, de acordo com que este, ou aquele, número seja da forma $4r+1$, pois o outro, sendo da forma $4r-1$, sempre será excluído.

522. Por exemplo, seja $p = 2m$ e seja $4m+1$ um número primo. Se $4q$ for um resíduo do divisor $4m+1$, então $4q+4m+1$ será resíduo do divisor $4(4m+1)$; mas, se $4q+2$ for resíduo do divisor $4m+1$, então $4q+2+3(4m+1)$ será resíduo do divisor $4(4m+1)$.

523. Seja $p = 2m-1$ e seja $4m-1$ um número primo. Se $4q$ for resíduo do divisor $4m-1$, então $4q+3(4m-1)$ será resíduo do divisor $4(4m-1)$. Mas, se $4q+2$ for resíduo do divisor $4m-1$, então $4q+2+4m-1 = 4q+4m+1$ será resíduo do divisor $4(4m-1)$.

524. Por meio destas regras para os vários resíduos do divisor $2p+1$, a mesma quantidade de resíduos do divisor $4(2p+1)$ é achada; pois, para cada caso, ou o próprio número, ou o mesmo aumentado por $2p+1$, ou $2(2p+1)$, ou $3(2p+1)$ fornecerá um número da forma $4q+1$, o que será resíduo do divisor $4(2p+1)$.

525. Mais ainda, de qualquer resíduo do divisor $2p+1$, determina-se também um não-resíduo, da forma $4q-1$, para o divisor $4(2p+1)$. E, de fato, de qualquer não-resíduo do divisor $2p+1$, produz-se dois não-resíduos para o divisor $4(2p+1)$; pois,

se aquele for par, somando[13] $2p+1$ e $3(2p+1)$, enquanto se ímpar, somando 0 e $2(2p+1)$, dois não-resíduos serão obtidos.

Sobre o divisor $8(2p+1) = d$.

526. Neste caso, sempre há oito números menores que d, cujos quadrados, divididos por d, deixam o mesmo resíduo, isto é, sendo a um desses números, os outros sete são

$$2(2p+1)\pm a,\ 4(2p+1)\pm a,\ 6(2p+1)\pm a,\ 8(2p+1)-a$$

e não pode ser exibido mais.

527. Visto que a quantidade de números menores que d e primos com ele é $= 4\cdot 1\cdot 2p = 8p$ e esses fornecem o mesmo resíduo de oito em oito, é claro que o número de resíduos distintos será $= p$, e o de não-resíduos $= 7p$.

528. Em seguida, é claro que qualquer número da forma $4q-1$, ou seja, tanto $8q-1$, quanto $8q-5$, não pode ocorrer entre os resíduos; nem é possível que qualquer número da forma $8q+5$ esteja entre os resíduos, pois a forma $xx-(8q+5)$ nunca pode ser dividido nem por 8, nem portanto por $8(2p+1)$, porque, devido ao fato que x é ímpar, $xx = 8n+1$.

529. Portanto, não há outros resíduos, exceto os da forma $8q+1$ e, porque o divisor é $16p+8$, todos os números de 0 até $2p$ podem ser tomados para n. Mas, tanto $2p+1$, quanto $3(2p+1)$,

[13] N. do Trad. No texto original, há $2(2p+1)$, em vez de $3(2p+1)$.

$5(2p+1)$ e $7(2p+1)$ são excluídos da forma $8n+1$ e, assim, restam apenas $2p$ desses números da forma $8n+1$, dos quais só metade constituem os resíduos.

530. Destes números da forma $8n+1$, cuja quantidade é $2p$, se um for um não-resíduo, o resto dos p não-resíduos será achado multiplicando cada resíduo por este; o restante dos números ímpares, seja da forma $8n+3$, ou $8n+5$, ou $8n+7$, fornecerá $6p$ não-resíduos[14].

531. Portanto, o divisor $8(2p+1)$ fornece a mesma quantidade de resíduos quanto o divisor $2p+1$; se esses forem 1, α, β, γ, δ, *etc*., os vários resíduos do divisor $8(2p+1)$ serão eliciados, somando múltiplos de $2p+1$ de tal maneira que a soma seja da forma $8n+1$, como pode ser visto no seguinte exemplo:

Para o divisor 13, resíduos	1, 3, 4, 9, 10, 12
Adicione	0, 6·13, 13, 0, 3·13, 13
para o divisor 104, resíduos	1, 81, 17, 9, 49, 25.

532. Se A for resíduo para o divisor $8(2p+1)$, então A^p-1 será divisível por $8(2p+1)$ e, se isto acontecer, A, por sua vez, será um resíduo dos quadrados.[15] Isto é, se A^p-1 for divisível por $8(2p+1)$, sempre será possível determinar um quadrado xx, tal que $xx-A$ será divisível por $8(2p+1)$.

[14] N. do Trad. O texto original tem "resíduos," em vez de "não-resíduos".
[15] N. do Trad. Ver §298 e §321.

Sobre o divisor $3(2p+1) = d$.

533. A quantidade de números menores que esse divisor[16] e primos com ele é $= 2 \cdot 2p = 4p$, entre os quais há pelo menos dois, a saber, a^2 e $(d-a)^2$, cujos quadrados deixam o mesmo resíduo; em consequência, o número de resíduos distintos não pode ser maior que $2p$.

534. Mais ainda, como a não é divisível por 3, ou $2p+1-2a$, ou $2(2p+1)-2a$, será divisível por 3. Seja o quociente $= m$. Então, o quadrado do número $3m+a$ deixará o mesmo resíduo[17] de ou $2p+1-a$, ou $2(2p+1)-a$, e, logo, ou $2(2p+1)+a$, ou $2p+1+a$ também deixará o mesmo resíduo.

535. Deste modo, visto que os quadrados deixam o mesmo resíduo de quatro em quatro[18], o número de resíduos diversos será apenas $= p$, o que é, portanto, o mesmo como para o divisor $2p+1$. Nenhum número da forma $3n-1$ pode estar entre os resíduos, visto que nenhum quadrado[19], diminuído por um número do referido tipo, pode ser dividido por 3, nem, portanto, por $3(2p+1)$.

[16] N. do Trad. É suposto aqui que $2p+1 > 3$.
[17] N. do Trad. Temos $(3m+a)^2 = (i(2p+1)-2a)(i(2p+1))+a^2$, onde $i = 1$ ou $i = 2$. Deve-se mostrar também que $3m+a$ é distinto de a e de $d-a$ (módulo d), o que, no entanto, não é difícil.
[18] N. do Trad. A saber: a, $d-a$, $3m+a$ e $d-(3m+a)$.
[19] N. do Trad. Todo quadrado perfeito tem a forma $3k$, ou a forma $3k+1$.

536. Portanto, todos[20] os resíduos do divisor $3(2p+1)$ terão a forma $3n+1$ e, se os resíduos do divisor $2p+1$ forem 1, α, β, γ, *etc*., escolhido qualquer que seja, ou ele próprio, ou o mesmo aumentado pelo número $2p+1$, ou $2(2p+1)$, resultará num número da forma $3n+1$ e será um resíduo do divisor $3(2p+1)$.

Para o divisor $(2p+1)(2q+1) = d$.

537. Sejam 1, α, β, γ, δ, *etc*. os resíduos para o divisor[21] $2p+1$, sendo sua quantidade = p, e sejam 1, π, ρ, σ, τ, *etc*. os resíduos para o divisor $2q+1$, sendo sua quantidade = q, então os números comuns a cada classe serão resíduos do divisor $d = (2p+1)(2q+1)$.

538. Mas, sendo o número $m(2p+1)+\alpha$ pertencente à primeira classe, m pode ser definido de tal forma que o referido número é igual ou a $n(2q+1)+1$, ou $n(2q+1)+\pi$, *etc*. e, desta modo, a partir de cada resíduo do divisor $2p+1$, q resíduos do divisor $2q+1$ são produzidos, de tal forma que, ao todo, pq resíduos distintos para o divisor $(2p+1)(2q+1)$ são obtidos.

539. Seja $5\cdot7 = 35$ o divisor composto deste tipo. Como os resíduos para o divisor 5 são dois, a saber, 1 e 4, enquanto para 7 são três, a saber, 1, 2 e 4, então para o divisor 35 os

[20] N. do Trad. No entanto, análogo ao caso anterior, nem todos os números menores que d e a ele primos, que também têm a forma $3n+1$, serão resíduos.
[21] N. do Trad. Aqui $2p+1$ e $2q+1$ são supostos números primos distintos.

resíduos serão os números $7n+1$, $7n+2$, $7n+4$ que são contidos ou na forma $5m+1$, ou na forma $5m+4$. Serão, portanto, esses seis: 1, 29; 9, 16; 4, 11.

540. Como há apenas pq resíduos distintos para o divisor $(2p+1)(2q+1)$, os quadrados fornecerão o mesmo resíduo de quatro em quatro; se um deles for = aa, as raízes dos outros três serão:

$$(2p+1)(2q+1)-a, \quad m(2p+1)-a, \quad n(2p+1)+a$$

tomando os números m e n, de tal modo que $m(2p+1)-2a$ e $n(2p+1)+2a$ pode ser dividido por $2q+1$, o que, devido ao fato de que $2p+1$ e $2q+1$ são primos entre si, sempre pode ser feito de tal forma que m e n são menores que $2q+1$.

Capítulo XV

Sobre os divisores de números da forma *xx+yy*

541. Em primeiro lugar, excluímos os casos em que x e y têm um divisor comum; pois, se o máximo divisor comum fosse $= \varphi$ e $x = p\varphi$ e $y = q\varphi$, de tal modo que p e q são primos entre si, teríamos $xx+yy = (pp+qq)\varphi\varphi$ e o problema dos divisores se reduziria ao de achar os da forma $pp+qq$.

542. Assim, sejam x e y primos entre si. Pode acontecer que $xx+yy$ seja um número primo, e, para examinar isto, talvez um único caso, o mais simples dos quais é 2, será suficiente. Mas, para $xx+yy$ ser um número primo, excluímos o caso em que ambos x e y são números ímpares.

543. Assim, pondo um deles par e o outro ímpar, é evidente que todos os números primos $xx+yy$ devem estar contidos na forma $4n+1$, de tal modo que nenhum número da forma $4n-1$ pode ser a soma de dois quadrados.

544. Mas, se x e y são números ímpares, isto é, $x = 2p+1$ e $y = 2q+1$, poderá ser que sua metade $\frac{xx+yy}{2} = 2pp+2p+2qq+2q+1$ seja um número primo. Na verdade, temos

$$2pp+2p+2qq+2q+1 = (p+q+1)^2+(p-q)^2,$$

de novo uma soma de dois quadrados, dos quais um é par e o outro ímpar e, por isto, a soma das raízes, $2p+1$, é ímpar.

545. Se a soma de dois quadrados $aa+bb$ for multiplicada por uma outra soma de dois quadrados $cc+dd$, o produto $(aa+bb)(cc+dd)$ será de novo a soma de dois quadrados, pois é = $(ac\pm bd)^2+(ad\mp bc)^2$, o que, devido à ambiguidade dos sinais, pode acontecer de duas maneiras.

546. Assim, surge a seguinte proposição recíproca: se a soma de dois quadrados $pp+qq$ admitir ser dividida pela soma de dois quadrados $aa+bb$, o quociente também será a soma de dois quadrados; a verdade disto, porém, não segue daquilo, mas requer uma demonstração própria.

547. Para fazer essa demonstração, primeiro estipulo que a forma $pp+qq$ seja divisível por $aa+bb$; qualquer que seja os números p e q, sempre podem ser reduzidos[1] a números menores que $aa+bb$ e até que $\frac{1}{2}(aa+bb)$ e, visto que $pp+qq$ é divisível por $aa+bb$, também acontece que

$$(\pm\alpha(aa+bb)\pm p)^2+(\pm\beta(aa+bb)\pm q)^2$$

é divisível.

548. Mas, se $\frac{pp+qq}{aa+bb}$ for a soma de dois quadrados $cc+dd$, ou seja[2], $p = ac+bd$ e $q = ad-bc$, tomando $p = ac+bd+\alpha(aa+bb)$ e $q = ad-bc+\beta(aa+bb)$, então $pp+qq$ certamente admitirá divisão por $aa+bb$ e o quociente será

$$= cc+dd+2\alpha(ac+bd)+2\beta(ad-bc)+(\alpha\alpha+\beta\beta)(aa+bb),$$

o qual também é a soma dos dois quadrados $(c+\alpha a-\beta b)^2+(d+\alpha b+\beta a)^2$.

---

[1] N. do Trad. Com efeito, Euler está considerando os referidos números módulo d, onde $d = a^2+b^2$.

[2] N. do Trad. Ver §545.

549. De fato, isto é o que foi pedido acima[3]. Assim, digo, em primeiro lugar, se o divisor $aa+bb$ for um número primo, pelo qual a forma $pp+qq$ é divisível, o quociente será a soma de dois quadrados. Embora isto seja verdadeiro em geral, isto é, também quando $aa+bb$ é um número composto, mesmo assim a demonstração deveria ser feita; é obtida a partir do presente caso.

550. Como a e b são números primos entre si, p pode ser dado por eles, de modo que $p = ma–nb$, e isto em um número infinito de maneiras. Ora, se tivermos $q = na+mb$, certamente teremos $\frac{pp+qq}{aa+bb} = mm+nn$; mas se não tivermos $q = na+mb$, pondo $q = na+mb+s$, teremos

$$pp+qq = (aa+bb)(mm+nn)+2s(na+mb)+ss.$$

551. Portanto, como $2s(na+mb)+ss$ é divisível por $aa+bb$, é necessário[4] que ou s, ou $s+2(na+mb)$ é divisível. No primeiro caso, pondo $s = t(aa+bb)$, teremos

$$\frac{pp+qq}{aa+bb} = mm+nn+t(t(aa+bb)+2(na+mb))$$
$$= mm+2mbt+ttbb+nn+2nat+aatt = (m+bt)^2+(n+at)^2,$$

e, portanto, a soma de dois quadrados.

[3] N. do Trad. Ver §546.
[4] N. do Trad. Observe que, para tanto, é necessário mostrar que s é coprimo com a^2+b^2.

552. No segundo caso, pondo $s+2(na+mb) = t(aa+bb)$, teremos $s = t(aa+bb)-2(na+mb)$ e, portanto, $\frac{pp+qq}{aa+bb} = mm+nn+tt(aa+bb)-2t(na+mb) = (m-bt)^2+(n-at)^2$, de modo que, em ambos os casos, o quociente será uma soma de dois quadrados.

553. Portanto, é demonstrado que, se $pp+qq$ for divisível pelo número primo $aa+bb$, o quociente também será uma soma de dois quadrados. Disto, se o quociente não fosse a soma de dois quadrados, o divisor não seria um número primo da forma $aa+bb$; isto é, se fosse primo, não seria da forma $aa+bb$, ou, se fosse da forma $aa+bb$, não seria primo. Mais ainda, é permitido permutar[5] as palavras quociente e divisor.

554. Para simplificar, vamos denotar pelas letras A, B, C, D, *etc*. números primos da forma $aa+bb$. Se a soma de dois quadrados $pp+qq$ for divisível por um produto de tais números ABC, o quociente também será a soma de dois quadrados. Pois, temos $\frac{pp+qq}{A} = rr+ss$, então

$$\frac{rr+ss}{B} = tt+uu, \text{ mas } \frac{tt+uu}{C} = xx+yy, \text{ e, em consequência,}$$

$$\frac{pp+qq}{ABC} = xx+yy.$$

[5] N. do Trad. Ver §555.

555. Portanto[6], se a soma de dois quadrados $pp+qq$ for divisível por um número que não é a soma de dois quadrados, o quociente, se for primo, não será a soma de dois quadrados e, se for composto, não será um produto de números primos, cada um dos quais é uma soma de dois quadrados.

556. Devido a isto, se a soma de dois quadrados $pp+qq$ tiver um fator que não seja uma soma de dois quadrados, será necessário que se ache, entre o restante dos fatores primos, pelo menos um que não seja a soma de dois quadrados.

557. Agora, portanto, investiguemos se a soma de dois quadrados $pp+qq$, primos entre si, pode ser dividido por algum número $\mathfrak{A}$, que não seja a soma de dois quadrados. Para tanto, tomamos $pp+qq$ a ser divisível pelo referido número $\mathfrak{A}$, então, também $(p-m\mathfrak{A})^2+(q-n\mathfrak{A})^2$ será divisível por $\mathfrak{A}$. (*).

(*). *Escrito na margem*. Cujas raízes, se p e q forem primos entre si, também serão primos entre si.

558. Portanto, será possível exibir a soma de dois quadrados do referido tipo, cujas raízes p e q são menores que

[6] N. do Trad. Pois, $\frac{pp+qq}{X} = rr+ss$ implica que $\frac{pp+qq}{rr+ss} = X$.

$\mathfrak{A}$, e até menores que $\frac{1}{2}\mathfrak{A}$; pois, se p e q forem maiores[7], como também $(\mathfrak{A}-p)^2+(\mathfrak{A}-q)^2$ deve admitir a divisão, teremos que essas raízes serão menores que $\frac{1}{2}\mathfrak{A}$.

559. Haverá, assim, uma soma de dois quadrados $pp+qq$, menores que $\frac{1}{2}\mathfrak{A}\mathfrak{A}$ (visto que temos $p < \frac{1}{2}\mathfrak{A}$ e $q < \frac{1}{2}\mathfrak{A}$), que é divisível pelo número $\mathfrak{A}$; pondo o quociente = $\mathfrak{B}$, o qual também, portanto, não será a soma de dois quadrados[8], ou haverá um fator do referido tipo, e teremos que $\mathfrak{B} < \frac{1}{2}\mathfrak{A}$.

560. Ora, visto que $pp+qq$ é divisível por $\mathfrak{B}$, poderá ser exibida uma soma de dois quadrados $rr+ss$, menor que $\frac{1}{2}\mathfrak{B}\mathfrak{B}$ e divisível por $\mathfrak{B}$, bem como um quociente $\mathfrak{C}$, que será menor que $\frac{1}{2}\mathfrak{B}$ e, igualmente, não será uma soma de dois quadrados; mas, visto que $rr+ss$ é divisível por $\mathfrak{B}$, haverá $tt+uu < \frac{1}{2}\mathfrak{C}\mathfrak{C}$, divisível por $\mathfrak{C}$ e um quociente $\mathfrak{D} < \frac{1}{2}\mathfrak{C}$, que, da mesma forma, não será uma soma de dois quadrados.

---

[7] N. do Trad. Isto é, se $\frac{1}{2}\mathfrak{A} < p < \mathfrak{A}$ e $\frac{1}{2}\mathfrak{A} < q < \mathfrak{A}$.

[8] N. do Trad. Ver §555. O resultado é para $\mathfrak{B}$ primo; a próxima cláusula aborda o caso em que $\mathfrak{B}$ é composto.

561. Assim, finalmente chega-se a uma soma de dois quadrados tão pequena quanto queira, que ainda seria divisível por um número que não é uma soma de dois quadrados e, visto que isto é absurdo[9], segue com necessidade que uma soma de dois quadrados, primos entre si, não é divisível por qualquer número que não seja uma soma de dois quadrados.

562. Proposto então um número primo qualquer da forma $4n+1$, devido ao fato de que -1, ou seja $4n$, está entre os resíduos dos quadrados[10], sempre pode ser exibida uma soma de dois quadrados por ele divisível; em consequência, segue que todos os números primos da forma $4n+1$ são somas de dois quadrados.

563. No entanto, visto que números da forma $4n-1$ nunca podem ser uma soma de dois quadrados[11], nenhuma soma de dois quadrados, primos entre si, pode ser dividida por qualquer numero do tipo $4n-1$.

564. Querendo uma demonstração mais sucinta do fato de que, se uma soma de dois quadrados $pp+qq$ for divisível por uma soma de dois quadrados $aa+bb$, será necessário que o quociente também seja uma soma de dois quadrados, tentaremos realizar o mesmo pelo seguinte raciocínio.

[9] N. do Trad. Aqui Euler usa o método de "descida ao infinito", inventado por Fermat.
[10] N. do Trad. Ver §333.
[11] N. do Trad. Ver §543.

565. Podemos supor que os números a e b, no divisor $aa+bb$, são primos entre si; pois, se não fossem primos entre si, serão reduzidos a isto pela remoção do fator comum[12]. Logo, $aa+bb$ será primo tanto a a, quanto a b. Em consequência, quaisquer que sejam os números p e q, eles podem ser representados assim:

$$p = m(aa+bb)\pm fa \quad \text{e} \quad q = n(aa+bb)\pm gb,$$

e isto pode ser feito em um número infinito de maneiras.

566. Assim, como $pp+qq$ é divisível por $aa+bb$, também $ffaa+ggbb$ será divisível por $aa+bb$. Mas, devido às referidas infinitas representações, devem acontecer todos os casos em que $ffaa+ggbb$ é divisível por $aa+bb$ e, portanto, é necessário que aconteça também o caso em que $g = f$, pois a divisão acontece nesse caso. (*)

(*). *Escrito na margem*. Aqui[13] é questionável se o caso $g = f$ segue por necessidade da divisibilidade da fórmula $pp+qq$. A dúvida é confirmada, pois sejam

$a = 7$, $b = 4$, $p = 17$, $q = 6$ e teremos $aa+bb = 65$, $pp+qq = 325$;

no entanto, não podemos ter $17 = 65m\pm 7f$ ao mesmo tempo que $6 = 65n\pm 4f$; em consequência, a demonstração deve ser rejeitada.

[12] N. do Trad. Isto é, o M.D.C.

[13] N. do Trad. Aqui Euler dá um contraexemplo, mostrando que a sua própria tentativa de demonstração tem uma falha. Também identifica corretamente a falha: o fato de que a fórmula contém um número infinito de casos não implica que contém todos os casos.

$\frac{17^2+6^2}{7^2+4^2} = 1^2+2^2$, embora em hipótese alguma é ou $17 = 1\cdot 7 \pm 2\cdot 4$, ou $17 = 2\cdot 7 \pm 1\cdot 4$.

567. Dado isto[14], teremos $p = m(aa+bb) \pm fa$ e $q = n(aa+bb) \pm fb$; de que fazemos

$$\frac{pp+qq}{aa+bb} = \left\{ \begin{matrix} mm(aa+bb) \pm 2fma \\ nn(aa+bb) \pm 2fnb \end{matrix} \right. + ff$$

e essa expressão é $= (f \pm ma \pm nb)^2 + (\pm na \mp mb)^2$ e, portanto, uma soma de dois quadrados.

568. Segue de imediato, portanto, que, se o quociente não seja uma soma de dois quadrados, o divisor não pode ter essa propriedade; ainda mais, o produto de dois números, dos quais um é a soma de dois quadrados e o outro não, não pode ser uma soma de dois quadrados.

569. Junto com as coisas que foram propostas a partir de §558, é completamente demonstrado que a soma de dois quadrados, primos entre si, não tem divisor algum, exceto os que são, eles próprios, somas de dois quadrados e, também, que todos os números primos da forma $4n+1$ são somas de dois quadrados.

[14] N. do Trad. Isto é, o resultado de que $g = f$ dado em §566, mas mostrado não ser necessário na nota escrito na margem.

570. Se um número qualquer N for uma soma de quadrados em duas maneiras diferentes, ou seja,

$$N = aa+bb = cc+dd;$$

então N não será primo. Pois, visto que temos $aa–cc = dd–bb$, teremos que $d+b = \frac{m(a+c)}{n}$ e $d–b = \frac{n(a-c)}{m}$ e, assim, $b = \frac{m(a+c)}{2n} - \frac{n(a-c)}{2m}$. Desta forma,

$$N = aa+bb = \frac{(mm+nn)}{4mmnn}(nn(a–c)^2+mm(a+c)^2) = \frac{(mm+nn)}{4mm}((a–c)^2+(b+d)^2),$$

onde o denominador da fração não[15] pode ser cancelado. (*)

(*). *Escrito na margem*. $(a+c)(a–c) = (b+d)(d–b) = pqrs$, $a+c = pq$, $a–c = rs$, $b+d = pr$, $d–b = qs$; $a = \frac{pq+rs}{2}$, $b = \frac{pr-qs}{2}$, $aa+bb = \frac{1}{4}(pp+ss)(qq+rr)$.

[15] N. do Trad. A proposição é, de fato, verdadeira. No entanto, visto que Euler não conseguiu eliminar a fração, sua demonstração não é válida.

Capítulo XVI

Sobre os divisores de números da forma $xx+2yy$

571. Dados x e y primos entre si, ou ambos são ímpares, ou somente um deles é par; portanto, ou x, ou y, será par. Assim, será proveitoso investigar os três casos que resultam dessas considerações, isto é, os casos que se apresentam em relação à paridade e imparidade dos números.

572. Se ambos os números x e y forem ímpares, seus quadrados terão a forma $8n+1$ e teremos que $xx+2yy$ é um número da forma $8n+3$; mas, se x for ímpar e y par, visto que

$$xx = 8m+1 \quad \text{e} \quad 2yy = 2\cdot 4n,$$

teremos que $xx+2yy$ é um número da forma $8n+1$.

573. Se x for par e y ímpar, pondo $x = 2z$, teremos $xx+2yy = 2(2zz+yy)$; ora, como y é ímpar, de acordo com que z for ou par ou ímpar, teremos ou

$$xx+2yy = 2(8n+1), \quad \text{ou} \quad xx+2yy = 2(8n+3).$$

574. Portanto, todo número contido na forma $xx+2yy$, sob condição de x e y serem primos entre si, ou, pelo menos, de não serem ambos pares, se for ímpar[1], pertencerá ou à forma $8n+1$, ou à $8n+3$; mas se esse número for par, será contido ou na forma $2(8n+1)$, ou à $2(8n+3)$, e, nesse último caso, sua metade, isto é, $2zz+yy$, também será um número da forma $xx+2yy$.

[1] N. do Trad. Isto é o número x^2+2y^2.

575. Logo, números que têm ou a forma $8n+5$, ou a forma $8n+7$ com certeza não são números da forma $xx+2yy$ e nem os duplos[2] daquelas formas serão contidos nesta. Em consequência, uma quantidade infinita de números não é contida em $xx+2yy$.

576. Ainda mais, o produto[3] de dois números desta forma é contido na mesma forma; pois, temos $(aa+2bb)(cc+2dd) = (ac\pm 2bd)^2+2(ad\mp bc)^2$ e, disto, é claro que dois produtos do referido tipo são contidos nesta forma.

577. Merece ser demonstrado agora que, se o número $pp+2qq$ pode ser dividido por $aa+2bb$, seu quociente também será desta forma. Observa-se aqui que, porque a e b são primos a $aa+2bb$, pode-se fazer, em um número infinito de maneiras,

$$p = m(aa+2bb)\pm fa \quad \text{e} \quad q = n(aa+2bb)\pm gb$$

e, portanto, $ffaa+2ggbb$ será divisível por $aa+2ggbb$.

578. Deste modo, sejam admitidas, como obtidas, todas as fórmulas $ffaa+2ggbb$ divididas por $aa+2bb$; assim,[4] o caso em que $gg = ff$, ou seja, em que $g = \pm f$, será ali contido. Disto, provém que

$$\frac{pp+2qq}{aa+2bb} = \begin{cases} mm(aa+2bb)\pm 2mfa \\ 2nn(aa+2bb)\pm 4ngb \end{cases} \quad +ff = (f\pm ma\pm 2nb)^2+2(mb\mp na)^2.$$

[2] N. do Trad. Isto é, $2(8n+5)$ e $2(8n+7)$.
[3] N. do Trad. Compre com §545.
[4] N. do Trad. Compare com §566.

579. Não obstante, aquilo, que admitimos como dado, pode ser confirmado. Sejam 1, α, β, γ, δ, *etc*. os resíduos que surgem da divisão dos quadrados pelo número $aa+2bb$. Então, tanto todos os quadrados, quanto $-2bb$ e -2, serão contidos nestes resíduos, e até o duplo de todo quadrado negativo, isto é, $-2, -2\alpha, -2\beta, -2\gamma$, *etc*.

580. Qualquer quadrado qq, dividido por $aa+2bb$, deixa algum resíduo, o qual, visto que se pode fazer $q = n(aa+2bb)\pm gb$, pode ser representado por $ggbb$, enquanto o resíduo surgido da divisão de $2qq$, pode ser representado por $2ggbb$; portanto, o quadrado pp, dividido por $aa+2bb$, deve deixar $-2ggbb$. Mas, $aagg$ pode ser colocado no seu lugar e, assim, os quadrados pp e $aagg$ deixam resíduos iguais e, assim, pode-se fazer

$$p = m(aa+2bb)\pm ag.$$

581. Mas, essa demonstração deve ser rejeitada, a não ser que $aa+2bb$ seja um número primo, pois se ele for primo, dado que $ffaa+2ggbb$ e $ggaa+2ggbb$ são divisíveis por $aa+2bb$, é necessário que $ff-gg$ é divisível e, portanto, também ou $f-g$, ou $f+g$; em qualquer caso, porque $aa+2bb$ é contido em uma das partes, obtemos ou $g = +f$, ou $g = -f$. Mas, essa conclusão não procede se $aa+2bb$ fosse um número composto, visto que, neste caso, $f-g$ poderia ser divisível por um dos seus fatores e $f+g$ pelo outro.

582. Se o número $pp+2qq$ puder ser dividido pelo número $\mathfrak{A}$, que não seja da forma $xx+2yy$, o quociente não será um número primo da forma $xx+2yy$ e, por isto, se o quociente for primo, não será da forma $xx+2yy$; mas, se for composto, com certeza, nem todos seus fatores primos terão essa forma.

583. Pois, sejam A, B, C, D, *etc*. números primos da forma $xx+2yy$. Se $pp+2qq$ for divisível por $ABCD$ *etc*., seu quociente certamente será da forma $xx+2yy$; portanto, se o quociente, ou se um dos multiplicadores[5], não fosse da forma $xx+2yy$, não seria possível que o outro fator seja um produto de números primos da referido tipo.

584. Assim, se $pp+2qq$ pode ser dividido pelo número $\mathfrak{A}$, excluído da forma $xx+2yy$, o quociente, se for primo, não será dessa forma, ou, se for composta, certamente terá fatores que não terão essa forma. (*)

(*). *Escrito na margem*. Portanto, $pp+2qq$ não pode ser dividido por número primo algum da forma $8n+5$ ou $8n+7$; em consequência, se os quadrados forem divididos por números dos referidos tipos, -2 será entre os não-resíduos.

Se $\frac{xx+nyy}{aa+nbb}$ = inteiro, teremos $\frac{bbxx-aayy}{aa+nbb}$ = inteiro[6] e $\frac{aaxx-nnbbyy}{aa+nbb}$ = inteiro.

[5] N. do Trad. Isto é, fatores.
[6] N. do Trad. Aqui, e na próxima equação, o texto original tem "int."

585. Sejam $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, *etc*. números primos excluídos da forma $xx+2yy$. Já vimos que $pp+2qq$ não pode ser $A\mathfrak{A}$, nem $AB\mathfrak{A}$, nem $ABC\mathfrak{A}$ e, por isto, é certo que haverá ou nenhum número[7], ou pelo menos dois números $\mathfrak{A}$, $\mathfrak{B}$, contidos entre os fatores primos do número $pp+2qq$.

586. Assim, ainda não pode ser concluído se um único fator, embora seja composto, de $pp+2qq$ tiver a forma $xx+2yy$, ou se tiver uma forma diferente dessa. Resta demonstrar que o número $pp+2qq$ não pode ser da forma $\mathfrak{AB}$, ou $A\mathfrak{AB}$, ou $AB\mathfrak{AB}$, embora se fosse, $\mathfrak{AB}$ certamente seria um número dessa forma.

587. Devemos também investigar se $pp+2qq$ pode ser dividido por um número $\mathfrak{A}$ que não é da forma $xx+2yy$ porque, se pudesse ser feito, faríamos $p < \frac{1}{2}\mathfrak{A}$ e $q < \frac{1}{2}\mathfrak{A}$, logo $pp+2qq < \frac{3}{4}\mathfrak{AA}$ e o quociente $< \frac{3}{4}\mathfrak{A}$, que seria ou um número não da forma $xx+2yy$, ou teria um tal fator $\mathfrak{B}$, e, visto que ele também seria um fator de $pp+2qq$, o menor número $\mathfrak{B}$ poderia ser determinado que é divisor de alguma forma $xx+2yy$, mas, como isto não pode ser feito, os números $pp+2qq$ não têm divisor primo alguma que não seja da forma $xx+2yy$.

[7] N. do Trad. Isto é, nenhum número da forma x^2+2y^2.

Este livro foi projetado pela equipe editorial da Editora
da Universidade Federal do Rio Grande do Norte.
Foi impresso em setembro de 2015.

Arquivo para a História da Teoria dos Números e da Lógica é uma coleção de trabalhos originais e traduções de obras clássicas referentes à história das duas referidas áreas da matemática. Na sua totalidade, a coleção pretende apresentar recursos para a delineação do desenvolvimento histórico das duas mencionadas áreas, o esclarecimento das relações existentes entre ekas e a investigação de como essas duas áreas se inseriram nos contextos históricos, não somente da Matemática em geral, mas também nos contextos históricos das culturas gerais das quais faziam parte nos vários estágios do seu desenvolvimento.

Volumes do *Arquivo* já publicados:

- Os Primórdios da Teoria dos Números
- Uma Investigação das Leis do Pensamento
- Um Estudo Histórico-Epistemológico do Conceito de Número Negativo
- Um Estudo sobre as origens da Lógica Matemática
- Tratado do Triângulo Aritimético
- Tratado sobre Triângulos Retângulos em Números Inteiros
- A Teoria dos Números de Adrien-Marie Legendre

Próximos Lançamentos:

- Sobre Números Amigáveis
- Investigação Sistemática e Propriedades dos Triângulos Retângulos em Números Inteiros

Associação Brasileira das Editoras Universitárias

9 788542 502763