Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

OS NÚMEROS PERFEITOS E OS PRIMOS DE MERSENNE

Tito José Minhava Botelho da Costa

Dissertação

Mestrado em Matemática para Professores

Orientador: Professor Doutor Pedro Freitas

2015

Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

OS NÚMEROS PERFEITOS E OS PRIMOS DE MERSENNE

Tito José Minhava Botelho da Costa

Dissertação

Mestrado em Matemática para Professores

2015

AGRADECIMENTOS

A conclusão deste trabalho só foi possível pela força, paciência e motivação transmitida por todos aqueles com quem mais diretamente interagi durante a sua realização.

Ao Professor Doutor Pedro Freitas, agradeço toda a paciência que teve no acompanhamento do trabalho, tantas vezes demorado. Agradeço a celeridade e objetividade das correções, assim como a pertinência das sugestões apresentadas.

Á minha esposa e filhas, agradeço a força que sempre me deram para concluir o trabalho. Sem elas não teria sido possível terminar esta dissertação pois foram muitos os momentos onde pensei em não o fazer, dada a sobrecarga de trabalho que a profissão docente atualmente acarreta, que absorve totalmente o tempo e a energia disponível para a realização de outros objetivos, em particular, os que se referem ao aprofundar do conhecimento matemático.

Finalmente, uma palavra de apreço para com as minhas colegas de curso que sempre se mostraram disponíveis para partilhar os materiais recolhidos durante as aulas do curso.

A todos, obrigado.

RESUMO

Os números e as suas regularidades desde sempre fascinaram os matemáticos. Ao longo dos tempos, a busca de provas ou refutações de várias conjeturas impulsionaram o avanço do conhecimento matemático, levando ao aparecimento da Teoria dos Números.

Muitos foram os matemáticos de renome que, em diferentes momentos históricos, deram o seu contributo para esta evolução. Mesmo as antigas civilizações Babilónia e Egípcia tinham já conhecimentos sobre os números, as suas propriedades e regularidades, apesar das escassas referências escritas existentes não permitirem aferir rigorosamente o quão profundo era esse conhecimento.

Já o mesmo não acontece com a civilização grega, cuja curiosidade, engenho e genialidade de alguns dos seus matemáticos se encontra bem documentada. O texto matemático mais importante da época grega foi, indubitavelmente, a obra de Euclides os *"Elementos"*, na qual, nos seus capítulos VII, VIII e IX, existem referências e provas de alguns resultados que revelam um profundo conhecimento da Teoria do Números, em particular, dos números perfeitos e dos números primos, cujas propriedades e regularidades apaixonaram os matemáticos em diferentes momentos.

Com este trabalho, pretendemos realizar uma súmula dos resultados e conjeturas mais relevantes referentes ao processo que alicerçou o estudo dos números perfeitos desde a antiguidade até aos dias de hoje.

Atualmente, a procura de números perfeitos resume-se a encontrar os denominados primos de Mersenne, isto é, primos da forma $2^n - 1$, cujo trabalho do monge minimita

Marin Mersenne mostrou estarem na base da factorização de todos os números perfeitos conhecidos.

Tentaremos ainda fazer referência a alguns dos desafios, que atualmente persistem, referentes aos números perfeitos e às suas propriedades, assim como de algumas conjeturas que, apesar de experimentalmente corroboradas com recurso aos meios computacionais atuais, ainda carecem de prova ou refutação.

ABSTRACT

Numbers and their regularities forever fascinated mathematicians. Throughout the ages, the search for evidence or refutations of several conjectures boosted the advancement of mathematical knowledge, leading to the appearance of number theory.

Many were the renowned mathematicians who, in different historical moments, contributed to this development. Even the ancient Babylonian and Egyptian civilizations had extensive knowledge about the numbers, their properties and regularities, in spite of the scarce written references which do not allow us to accurately gauge how deep was this knowledge.

The same is not true with the Greek civilization, win which curiosity, resourcefulness and genius of some of their mathematicians is well documented. The most important mathematical text of that time was, undoubtedly, the work of Euclid's *"Elements"*, in which, in chapter IX, there are references and evidence of some results which reveal a deep knowledge of the theory of numbers, in particular, of perfect and prime numbers, whose properties and regularities fascinated mathematicians at different times.

With this work, we intend to present a collection of results and conjectures there were more relevant for the process that allowed the study of perfect numbers from antiquity to the present day.

Currently, the demand for perfect numbers resumes itself to find what is now known as Mersenne primes, in honor of the monk Marin Mersenne that, among others results, showed

that primes numbers that can be written in the form $2^n - 1$ are factors in the factorization of all known perfect numbers.

We also intend to make reference to some of the challenges that currently persist in the study of perfect numbers and their properties, as well as some conjectures that, although experimentally corroborated with current computational means, still lack proof or refutation.

ÍNDICE

INTRODUÇÃO

A procura e o estudo dos números perfeitos é antiga e passa por muitos matemáticos ao longo do tempo. Começa com a descoberta destes números por volta do ano 540 a.C., durante a influência da escola pitagórica. Estes acreditavam que o número era o conceito fundamental do universo. Classificavam os números de diversas formas: números figurados, primos, amigos, triangulares, etc.

Um dos seus conceitos fundamentais, era a definição de número primo, dado que era a partir destes que podiam escrever todos os outros. Outra classificação que revela propriedades interessantes era a classificação de perfeição de um número. Este podia ser considerado *deficiente* se a soma dos seus divisores, com exceção do próprio, fosse menor que o próprio número. Era classificado como *abundante* se a referida soma fosse superior ao próprio número. Caso a soma dos divisores de um número, com exceção do próprio, coincidisse com o próprio número, este era considerado perfeito.

Com estas classificações, os pitagóricos procuravam encontrar propriedades especiais para cada tipo de números, busca que foi continuada por muitos outros matemáticos ao longo da história.

Após os pitagóricos, o próximo matemático a contribuir significativamente para o estudo dos números perfeitos foi Euclides (aproximadamente 300 a.C.). Das várias

referências feitas por Euclides relativamente aos números perfeitos na sua obra *"Elementos"*, destaca-se a seguinte proposição:

> *"(…)Se tantos números quantos se queira, começando a partir da unidade, forem dispostos continuamente numa proporção duplicada até que a soma de todos resulte num número primo, e se a soma multiplicada pelo último origina algum número, então o produto será um número perfeito.(…)"*

Utilizando linguagem matemática atual, este excerto significa que se um número da forma $2^n - 1$ é primo, então o número $2^{n-1}(2^n - 1)$ é um número perfeito.

Tal resultado facilitou a procura de números perfeitos, sendo na realidade a primeira fórmula encontrada para o seu cálculo.

Os gregos antigos só conheciam os primeiros quatro números perfeitos: 6, 28, 496 e 8128, números estes que podem ser obtidos a partir da fórmula de Euclides utilizando para *n* os números 2, 3, 5 e 7 respetivamente.

Com base nestes valores, o neo-pitagórico Nicómaco (aproximadamente 100 d.C.) fez algumas afirmações referentes aos números perfeitos. Por exemplo, afirmou que se 6 tinha um dígito, 28 tinha dois, 496 tinha três e 8128 tinha quatro, o próximo número perfeito teria cinco dígitos. Afirmou também que o próximo número perfeito seria gerado a partir do primo 11, já que os primeiros quatro haviam sido gerados pelos primeiros quatro números primos. Referiu ainda que os números perfeitos terminavam, alternadamente, em 6 e 8.

Todas estas conjeturas de Nicómaco foram refutadas com a descoberta dos números perfeitos seguintes. O quinto número perfeito foi descoberto no século XV, 33550336, o que derrubou as duas primeiras conjeturas referidas visto ser gerado pelo primo 13 e não ter cinco algarismos. Aquando da descoberta do sexto número perfeito, 8589869056, foi refutada a última conjetura referida uma vez que, tal como o seu antecessor, termina em 6.

Por volta do ano 1000 d.C., o matemático Alhazem percebeu que a proposição de Euclides era válida para números perfeitos pares, isto é, se um número perfeito era par então ele era da forma $2^{n-1}(2^n-1)$, apesar de não ter conseguido demonstrá-lo.

Alhazem estava correto, mas foi apenas durante o século XVIII que surgiu a demonstração desse resultado, apresentada pelo matemático suíço Leonhard Euler. Tendo sido um dos matemáticos mais produtivos de todos os tempos, Euler serviu de inspiração para muitos outros, em particular Pierre Fermat que, apesar de não ser matemático de profissão, também estudou as propriedades dos números perfeitos, trabalho esse que originou, entre outros, o teorema que ficou conhecido como "Pequeno Teorema de Fermat".

Com a demonstração apresentada por Euler, a procura de mais números perfeitos resumiu-se à busca de número primos da forma 2^n-1, mais conhecidos por primos de Mesenne, nome dado em homenagem a Marin Mersenne, matemático que dedicou a sua obra à procura destes números.

Mais recentemente, o matemático Edouard Lucas, teve um papel de relevo na busca por mais números perfeitos. Provou que todos os números perfeitos pares terminam em 16, 28, 36, 56, 76 ou 96. Além disso, mostro que $2^{127}-1$ é primo, descobrindo deste modo o maior número perfeito antes da era dos computadores.

Com o surgimento dos computadores e dos supercomputadores, outros números perfeitos foram encontrados. Atualmente são conhecidos 47 primos de Mersenne e, por consequência, 47 números perfeitos, o maior dos quais tem 12978189 algarismos tendo sido descoberto em 2009. Até hoje não foi encontrado mais nenhum.

Apesar de todos os recursos tecnológicos disponíveis, questões como a existência de um número perfeito ímpar ou a infinidade dos números perfeitos continuam em aberto, despertando a curiosidade e aguçando o engenho dos matemáticos de hoje e do amanhã.

CAPÍTULO I

I. RESULTADOS DA TEORIA DOS NÚMEROS

Ao longo deste trabalho far-se-ão várias referências a diversas definições e resultados da Teoria dos Números. Deste modo, é nosso objetivo neste primeiro momento realizar uma pequena compilação das principais referências que serão posteriormente utilizadas aquando da abordagem dos diferentes temas.

I.1. NÚMEROS PRIMOS

Muitos são os resultados importantes sobre as propriedades dos números primos. Seguidamente apresentamos aqueles dos quais necessitaremos neste trabalho.

Não poderíamos deixar de começar pelo teorema fundamental da aritmética.

Já o matemático grego Euclides, na sua obra os *"Elementos"*, para além de o enunciar, praticamente o demonstra. A primeira demonstração formal escrita é atribuída a Gauss.

Teorema 1

Qualquer número natural $n>1$ escreve-se de uma única forma como produto de fatores primos.

Demonstração

Seja $n>1$, número natural.

Se *n* for primo o resultado é imediato visto podermos encará-lo como produto de um só fator.

Se *n* for composto, então *n* tem divisores entre 1 e *n*. Seja *m* o menor desses divisores. Este tem de ser necessariamente primo, pois caso contrário existiriam divisores de *m*, e por consequência de *n*, menores que *m*.

Seja então $m=p_1$.

Temos $n=p_1a_1$, com p_1 primo e $1<a_i<a$.

Se a_1 for primo, obtemos a conclusão desejada. Caso contrário, repetindo o raciocínio anterior, a_1 tem um divisor primo p_2, com $1<p_2<a_1$ tal que $n=p_1p_2a_2$ e com p_1, p_2 primos e $1<a_2<a_1<a$.

Deste modo obtemos uma sucessão de números naturais $a>a_1>a_2>\ldots$. Como uma sucessão de números naturais não pode decrescer indefinidamente, há-de haver um momento em que um destes números é primo, digamos p_s, ou seja $a=p_1p_2\ldots p_s$.

Verificámos então que qualquer número natural pode ser escrito como produto de fatores primos. Resta ver que essa decomposição é única.

Suponhamos, com vista a um absurdo, que *a* pode ser escrito de duas formas distintas como produto de fatores primos, ou seja,

$$a=p_1p_2\ldots p_s=q_1q_2\ldots q_t.$$

Podemos então simplificar estas factorizações de a de modo a que não existam fatores comuns, ou seja, de modo a que não haja nenhum primo que figure em ambos os membros.

Como p_1 divide o primeiro membro, divide também o segundo, ou seja, $p_1 \mid q_1 q_2 ... q_t$, o que significa que $p_1 \mid q_j$, para algum $j \in \{1,...,t\}$. Como ambos são primos, temos de ter $p_1 = q_j$, o que contradiz o facto de não poderem existir primos comuns nas duas factorizações.

Logo qualquer número natural $n > 1$, escreve-se de uma única forma como produto de fatores primos. □

Como veremos, a procura de números primos da forma $2^k - 1$ está historicamente relacionada com o desenvolvimento da teoria dos números, pelo que uma análise mais cuidada de alguns resultados a eles associados é imperativa.

Lema 1

Sejam a, k naturais. Temos $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$.

Demonstração

Sejam a, k naturais. Verifiquemos que $a^k - 1$ admite a seguinte factorização: $(a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$.

$$(a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1) =$$
$$= a \cdot a^{k-1} + a \cdot a^{k-2} + \cdots + a^2 + a - a^{k-1} - a^{k-2} + \cdots - a - 1 =$$
$$= a^k + \cancel{a^{k-1}} + \cdots + \cancel{a^2} + \cancel{a} - \cancel{a^{k-1}} - \cancel{a^{k-2}} - \cdots - \cancel{a^2} - \cancel{a} - 1 =$$
$$= a^k - 1$$

Logo, $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$. □

Deste modo, estamos em condições de mostrar que se $2^k - 1$ é primo, então *k* tem de ser ele próprio um número primo. De uma forma mais geral, temos os seguinte teorema:

Teorema 2

Sendo *a*, *k* números naturais com $k > 1$ e $a^k - 1$ primo, então $a = 2$ e *k* é primo.

Demonstração

Se $a = 1$, resulta que $a^k - 1 = 1^k - 1 = 0$, donde $a^k - 1$ não é número primo, o que contradiz a hipótese. Logo $a \geq 2$.

Suponhamos agora que $a > 2$ e $k \geq 2$.

Como $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$, teríamos que $a^k - 1$ admitiria uma factorização com fatores diferentes de um e do próprio, o que contradiz a hipótese de $a^k - 1$ ser primo.

Logo, temos que $a = 2$.

Assim, se $k = 1$ então teríamos $a^k - 1$ não primo dado que $a^k - 1 = 1$.

Suponhamos agora, com vista a um absurdo, que *k* é um número composto, ou seja, que existem *m*, *n* naturais tais que $k = m \cdot n$, com $m, n > 1$.

Então $a^k - 1 = a^{mn} - 1 = (a^m)^n - 1 = (a^m - 1)((a^m)^{n-1} + (a^m)^{n-2} + \cdots + a^m + 1)$.

Ora, como $a = 2$ e $m > 1$, temos que, por um lado, que $a^m - 1 > 1$, e por outro que $(a^m)^{n-1} + (a^m)^{n-2} + \cdots + a^m + 1 \geq a^m + 1 \geq 2$, o que significa que $a^k - 1$ admite um a factorização com fatores diferentes de um e do próprio, o que contradiz a hipótese de $a^k - 1$ ser primo.

Deste modo concluímos que *k* tem de ser primo. □

Muitos autores antigos acreditavam que $2^p - 1$ seria primo para qualquer *p* primo considerado.

Em 1536, Hudalrichus Regius apresentou a factorização de $2^{11} - 1 = 2047 = 23 \cdot 89$ com recurso a um ábaco demonstrando que a convicção estava incorreta.

I.2. RESULTADOS SOBRE CONGRUÊNCIAS

Outra peça fundamental da nossa exploração serão as relações de congruência.

Tentando não ser demasiado minimalistas no que respeita aos conteúdos a salientar, teremos indubitavelmente de começar por definir relação de congruência entre dois números inteiros, assim como analisar algumas das suas propriedades.

Deste modo, diremos que dois números inteiros *a* e *b* são congruentes para o módulo *m*, inteiro não nulo, quando divididos por *m* derem o mesmo resto. Notaremos esta relação como $a \equiv b \pmod{m}$, que se lê *a* congruente com *b* módulo *m*. Passaremos igualmente a notar *m* divide *a* por $m \mid a$.

Desta definição, resulta imediatamente que, se $a \equiv b \pmod{m}$, então $a - b$ é múltiplo de *m*, ou seja, que $m \mid (a - b)$.

Como facilmente se pode constatar, a relação de congruência é:

- reflexiva [$a \equiv a \pmod{m}$];
- simétrica [$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$];
- transitiva [$a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$].

Temos ainda que, dados os inteiros a, a', b, b' e m natural não nulo tais que $a \equiv a' (\mathrm{mod}\, m)$ e $b \equiv b' (\mathrm{mod}\, m)$, a relação de congruência respeita a soma e a multiplicação algébrica, ou seja:

- $a \pm b \equiv a' \pm b' \pmod{m}$;
- $ab \equiv a'b' \pmod{m}$.

Tendo por base as propriedades anteriormente enunciadas, podemos agora provar alguns resultados.

Teorema 3

Sendo p primo, e a, b inteiros quaisquer tais que $ab \equiv 0 \pmod{p}$, então $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$.

Demonstração

Consideremos a seguinte decomposição de a e de b em fatores primos: $a = p_1^{a_1} \cdots p_i^{a_i}$ e $b = q_1^{b_1} \cdots q_j^{b_j}$.

Temos então que $ab = p_1^{a_1} \cdots p_i^{a_i} \cdot q_1^{b_1} \cdots q_j^{b_j}$, com p_i e q_j não necessariamente todos distintos.

Se $ab \equiv 0 \pmod{p}$, então $p \mid ab \Leftrightarrow p \mid p_1^{a_1} \cdots p_i^{a_i} \cdot q_1^{b_1} \cdots q_j^{b_j}$. Como p é primo, temos que $p = p_i$, para algum i, ou, $p = q_j$, para algum j.

Se $p = p_i$, para algum i, temos que $p \mid p_1^{a_1} \cdots p_i^{a_i} \Leftrightarrow p \mid a$. Se $p = q_j$, para algum j, temos que $p \mid q_1^{b_1} \cdots q_j^{b_j} \Leftrightarrow p \mid b$.

Ou seja, se p é primo e $p \mid ab \Leftrightarrow p \mid a \vee p \mid b$. □

Este resultado equivale a dizer que *p* primo, e *a*, *b* inteiros quaisquer tais que $ab \equiv 0 \pmod{p}$ se e só se $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$, ou seja, podemos dizer que sendo *p* primo e *a*, *b* inteiros quaisquer, a condição necessária e suficiente para que $p \mid ab$ é $p \mid a$ ou $p \mid b$.

Deste modo, vários resultados e propriedades dos números surgem e demonstram-se naturalmente.

O teorema seguinte é um desses casos e utilizar-mo-emos no próximo capítulo deste trabalho.

Teorema 4

Seja *k* um número ímpar qualquer. Então $k \equiv 1 \pmod{4}$ ou $k \equiv 3 \pmod{4}$.

Demonstração

Temos que, qualquer que seja o número natural considerado, só existem quatro restos possíveis na divisão por quatro, a saber, 0, 1, 2 ou 3.

Seja *k* um número ímpar qualquer.

Se $k \equiv 0 \pmod{4} \Leftrightarrow k = 4j$, para algum $j \in \mathbb{N}$, donde resulta que *k* é par, o que contradiz a hipótese de *k* ser ímpar.

Se $k \equiv 2 \pmod{4} \Leftrightarrow k = 4i + 2 \Leftrightarrow k = 2(2i + 1)$, para algum $i \in \mathbb{N}_0$, donde resulta que *k* é par, o que contradiz a hipótese de *k* ser ímpar.

Logo resulta que $k \equiv 1 \pmod{4}$ ou $k \equiv 3 \pmod{4}$. □

Muitíssimo mais poderia ser referenciado sobre congruências, mas o nosso objetivo neste ponto é unicamente destacar os resultados que mais tarde utilizaremos.

I.3. RESULTADOS ARITEMÉTICOS

Importa igualmente analisar alguns dos resultados, assim como algumas definições, relativas aos números naturais em geral.

Associada à noção de número primo, surge a definição de números primos entre si, também conhecidos por números coprimos.

Definição 1

Sejam *m*, *n* dois números naturais. Estes dizem-se coprimos se o único número natural que os divide simultaneamente for o um.

A análise dos divisores comuns entre números naturais originou todo um conjunto de resultados significativos para o conhecimento matemático, em particular, o facto do divisor comum entre dois números naturais poder ser escrito como combinação linear deste mesmos dois números. Um dos processos para obter essa combinação linear ficou conhecido como algoritmo de Euclides, utilizado na demonstração do resultado seguinte.

Teorema 5

Sejam *b* e *c* inteiros não ambos nulos, e seja *d* o seu máximo divisor comum. Então existem inteiros x_0 e y_0 tais que $d = bx_0 + cy_0$.

Demonstração

Consideremos o conjunto $C = \{bx + cy : x, y \in \mathbb{Z}\}$.

Seja *t* o menor inteiro positivo de *C*. Então, para certos inteiros x_0 e y_0, $t = bx_0 + cy_0$. Vejamos que $t = d$.

Comecemos por mostrar que $t \mid b$. Dividindo *b* pot *t*, obtermos $b = qt + r$, com $0 \le r < t$. Assim, $r = b - qt = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$, ou seja, *r* é um elemento do conjunto *C*. Se *r* fosse positivo, teria de ser um elemento de *C* positivo menor do que *t*, o que seria absurdo pela definição de *t*. Logo *r* tem de ser zero, o que significa que a divisão de *b* por *t* é exata, isto é, $t \mid b$.

Analogamente se prova que $t \mid c$.

Logo *t* é divisor comum de *b* e de *c*. Para vermos que $t = d$ basta observar que *d*, sendo um divisor comum de *b* e *c*, tem que dividir $bx_0 + cy_0$, ou seja, tem de dividir *t*. Logo tem-se $d \le t$.

Como *d* é o máximo divisor comum de *b* e *c*, tem que ser $d = t$. □

Deste modo, estamos em condições de analisar uma outra propriedade dos números naturais, associada à noção de números coprimos e de divisibilidade.

Propriedade 1 (Lema de Euclides)

Sejam a,b,c números naturais. Se $c \mid ab$ e *b* e *c* forem coprimos, então $c \mid a$.

Demonstração

Como $c \mid ab$ existe um inteiro *q* tal que $ab = qc$. Por outro lado, se *b* e *c* coprimos, existem inteiros *x* e *y* tais que $bx + cy = 1$.

Assim,

$$a = a(bx + cy) = abx + acy = qcx + acy = (qx + ay)c$$

donde resulta que $c \mid a$. □

Certas aplicações são de especial importância aquando do estudo dos divisores de um número inteiro.

Entre as mais simples e que surgiram mais naturalmente estão as aplicações tau e sigma que a seguir se definem.

Definição 2

Sendo *n* um número natural, designaremos por $\tau(n)$ o número de divisores positivos de *n*, incluindo o 1 e o *n*. □

Definição 3

Seja *n* um número natural. Denotaremos por $\sigma(n)$ a soma dos divisores de *n*, ou seja, $\sigma(n) = \sum_{i=1}^{\tau(n)} a_i$, com $a_i \mid n$, $\forall i \in \{1,...,\tau(n)\}$.

Também a análise de algumas das propriedades das aplicações que facilitam o estudo dos números inteiros é de especial relevância para este trabalho.

A noção de aplicação multiplicativa é transversal a muitos dos resultados na teoria dos números.

Definição 4

Seja $f(n)$ uma aplicação. $f(n)$ diz-se multiplicativa se para *m* e *n* naturais coprimos, temos $f(m \cdot n) = f(m) \cdot f(n)$.

Neste momento, definas as aplicações tau e sigma, assim como o conceito de aplicação multiplicativa, exploraremos algumas das suas propriedades.

Comecemos pela aplicação $\sigma(n)$.

Propriedade 2

$\sigma(n)$ é uma aplicação multiplicativa.

Demonstração

Para mostrarmos que σ é multiplicativa, temos que verificar que, para *m* e *n* naturais coprimos, temos $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$.

Sendo *m* e *n* coprimos, qualquer divisor de *mn* escreve-se de forma única como $d = d'd''$, com d' divisor de *m* e d'' divisor de *n*, isto porque não existem primos comuns nas factorizações de *m* e de *n*.

Reciprocamente, dados d' divisor de *m* e d'' divisor de *n*, resulta de imediato que o produto $d = d'd''$ é divisor de *mn*. Logo existe uma bijeção entre o conjunto dos divisores *d*

de *mn* e o conjunto dos pares (d', d'') em que d' é divisor de *m* e d'' é divisor de *n*, sendo cada elemento do primeiro conjunto igual ao produto dos elementos do par que lhe corresponde no segundo conjunto.

Sejam $d_1, d_2, ..., d_{\tau(mn)}$ os divisores de *mn*, $d'_1, d'_2, ..., d'_{\tau(m)}$ os divisores de *m* e $d''_1, d''_2, ..., d''_{\tau(n)}$ os divisores de *n*. Temos então que

$$\sigma(mn) = d_1 + d_2 + \cdots + d_{\tau(mn)}.$$

Como cada uma destas parcelas é igual os produto de um divisor de *m* por um divisor de *n*, tem-se que $\sigma(mn)$ é igual á soma de todos os possíveis produtos desta forma, isto é,

$$\begin{aligned}\sigma(mn) &= d'_1 d''_1 + d'_1 d''_2 + \cdots + d'_1 d''_{\tau(n)} + \\ &+ d'_2 d''_1 + d'_2 d''_2 + \cdots + d'_2 d''_{\tau(n)} + \cdots + \\ &+ d'_{\tau(m)} d''_1 + d'_{\tau(m)} d''_2 + \cdots + d'_{\tau(m)} d''_{\tau(n)} = \\ &= d'_1 \sigma(n) + d'_2 \sigma(n) + \cdots + d'_{\tau(m)} \sigma(n) = \sigma(m)\sigma(n)\end{aligned}$$

Logo, a aplicação $\sigma(n)$ é multiplicativa. □

Aplicando $\sigma(n)$ a números primos, todo um conjunto de resultados surge, dos quais destacamos os seguintes dois:

Propriedade 3

Se *p* for um número primo, $\sigma(p) = p + 1$.

Demonstração

Este resultado é imediato. Se *p* é primo, admite unicamente os divisores 1 e *p*, donde $\sigma(p) = p + 1$. □

Propriedade 4

Seja *n* um número natural maior do que um e seja $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a sua factorização como produto de números primos.

Então tem-se:

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right).$$

Demonstração

Comecemos por observar que, para qualquer número natural *n* maior do que um, $1 + n + n^2 + \cdots + n^\alpha$ corresponde á soma dos $\alpha + 1$ primeiros termos de uma progressão geométrica de razão *n*, e como tal, temos que

$$1 + n + n^2 + \cdots + n^\alpha = \frac{n^{\alpha+1} - 1}{n - 1}.$$

Por outro lado, sendo *p* um número primo, os divisores de p^α são exatamente as potências de *p* até ao expoente α, ou seja, $1, p, p^2, ..., p^\alpha$, donde resulta imediatamente que

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Assim, como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e a função $\sigma(n)$ é multiplicativa, temos

$$\sigma(n) = \sigma(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \cdots \sigma(p_k^{\alpha_k}) =$$
$$= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right). \qquad \square$$

A busca e constatação de regularidades associadas ao números inteiros originaram toda uma panóplia de critérios, mais ou menos simples, para o estudo e análise das propriedades dos números.

Em particular, determinaram-se formas simples de verificar a divisibilidade de um número por outro. Dos vários critérios de divisibilidade conhecidos, analisaremos o critério de divisibilidade por quatro, que terá relevância aquando do estudo dos números primos.

Propriedade 5

Seja *n* um número natural. O número *n* é divisível por quatro sse quatro divide o número formado pelos dois últimos algarismos de *n*.

Demonstração

Seja $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Se $k \in \{0,1,2\}$ o resultado é imediato.

Seja $k > 2$. Então,

$$\begin{aligned} n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = \\ = \left(a_k \cdot 10^{k-2} + a_{k-1} \cdot 10^{k-3} + \cdots + a_2\right) \cdot 10^2 + a_1 \cdot 10 + a_0 = \\ = \left(a_k \cdot 10^{k-2} + a_{k-1} \cdot 10^{k-3} + \cdots + a_2\right) \cdot 25 \cdot 4 + a_1 \cdot 10 + a_0 \equiv \\ \equiv 0 + a_1 \cdot 10 + a_0 = a_1 \cdot 10 + a_0 \pmod 4 \end{aligned}$$

Portanto, $4 \mid n \Leftrightarrow 4 \mid (a_1 \cdot 10 + a_0)$. □

I.4. RESULTADOS SOBRE CONGRUÊNCIAS

Dado que alguns dos resultados que exploraremos no capítulo seguinte são um pouco mais técnicos, importa relevar alguns conceitos e propriedades das relações de congruência, nomeadamente a noção de sistema de resíduos e algumas das suas propriedades.

Definição 5

Seja $m \in \mathbb{N}$. Um conjunto de *m* inteiros que se obtém escolhendo um único elemento de cada classe de congruência módulo *m* denomina-se por sistema completo de resíduos módulo *m*.

Definição 6

Seja $m \in \mathbb{N}$. Se de um sistema completo de resíduos módulo *m*, considerarmos o subconjunto formado pelos resíduos coprimos com *m*, obtemos o denominado sistema reduzido de resíduos módulo *m*. O número de elementos de qualquer sistema reduzido de resíduos designa-se por $\varphi(m)$.

A aplicação $\varphi(m)$ anteriormente definida é conhecido como aplicação fi de Euler, em homenagem ao seu criador, apesar de a notação $\varphi(m)$ ter sido introduzida posteriormente por Gauss.

Tratando-se de uma importante aplicação associada à teoria dos números, apresentaremos alguns dos resultados a ela associados.

Proposição 1

Dado $m \in \mathbb{N}$, tem-se que $\varphi(m)$ é igual ao número de naturais não superiores a *m* que são coprimos com *m*. Deste modo, um número natural *p* é primo se e só se $\varphi(p) = p - 1$.

Demonstração

Consideremos o sistema completo de resíduos módulo *m* $\{1, 2, ..., m\}$. Se considerarmos o sistema reduzido de resíduos que dele resulta obtemos imediatamente que $\varphi(m)$ é igual ao número de naturais não superiores a *m* que são coprimos com *m*. □

Proposição 2

Seja $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo *m* e seja *a* um inteiro coprimo com *m*. Então $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo *m*.

Demonstração

Por definição de sistema reduzido de resíduos, temos que *m* coprimo com r_i para $\forall i \in \{1, 2, ..., \varphi(m)\}$. Por outro lado, *m* é coprimo com *a*, donde resulta que *m* não tem fatores primos comuns com r_i nem com *a*, ou seja, *m* não tem fatores primos comuns com ar_i. Deste modo *m* é coprimo com ar_i, $\forall i \in \{1, 2, ..., \varphi(m)\}$.

No conjunto $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ não existem dois elementos congruentes módulo *m*. Se $ar_i \equiv ar_j (\mathrm{mod}\, m)$, como *a* e *m* são coprimos, teríamos $r_i \equiv r_j (\mathrm{mod}\, m)$, o que não pode acontecer visto $\{r_1, r_2, ..., r_{\varphi(m)}\}$ ser um sistema reduzido de resíduos módulo *m*.

Então no conjunto $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ temos $\varphi(m)$ inteiros, coprimos com *m* e não congruentes dois a dois módulo *m*. Ou seja, $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo *m*. □

Entre muitos outros resultados não provados, Fermat afirmou que se um número primo *p* não dividir um número inteiro *a*, então $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Apenas em 1936, Euler apresentou um demonstração deste resultado que ficou conhecido como pequeno teorema de Fermat.

Posteriormente, em 1760, Euler conseguiu generalizar o resultado apresentado por Fermat.

Teorema 6 ("Teorema de Euler")

Seja $m \in \mathbb{N}$. Se *a* é um inteiro coprimo com *m* então $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Demonstração

Seja $\{r_1, r_2, ..., r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo *m*. Temos então que $\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo *m*[1]. Deste modo, para cada elemento ar_i do segundo sistema, existe um e um só elemento r_j do primeiro sistema tal que $ar_i \equiv r_j (\mathrm{mod}\, m)$.

Multiplicando membro a membro todas as $\varphi(m)$ congruências anteriores obtemos

[1] *Proposição 2*

$$ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m) \Leftrightarrow$$
$$\Leftrightarrow a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m).$$

Como todos os r_i são coprimos com *m*, também o seu produto é coprimo com *m*, pelo que $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$. □

Corolário 1 ("Pequeno Teorema de Fermat")

Seja *a* um inteiro e seja *p* um número primo. Se *p* não dividir *a* então $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Não será certamente abusivo afirmar que estes dois últimos resultados são fundamentais para a teoria dos números, servindo de suporte e referência para muitos outros resultados e propriedades.

Neste momento, importa introduzir um novo conceito, o de ordem de um número inteiro.

Definição 7

Seja *a* um número inteiro coprimo com *m*. Denomina-se por ordem de *a* o menor inteiro *k* tal que $a^k \equiv 1 (\mathrm{mod}\, m)$ e representa-se por *ord(a)*.

Pelo teorema de Euler, $\varphi(m)$ é um inteiro nas condições da definição anterior, pelo que é sempre possível determinar a ordem de um número inteiro *a* coprimo com *m*.

Da definição de ordem, resulta a seguinte propriedade:

Proposição 3

Seja *k* tal que $a^k \equiv 1 (\mathrm{mod}\, m)$. Então $ord(a) \mid k$.

Demonstração

Efetuando a divisão inteira de *k* por *ord(a)*, obtemos $k = q \cdot ord(a) + r$, com $r < ord(a)$.

Deste modo

$$1 \equiv a^k = a^{q \cdot ord(a) + r} = \left(a^{ord(a)}\right)^q \cdot a^r \equiv 1^q \cdot a^r = a^r,$$

donde concluímos que $a^r \equiv 1 (\mathrm{mod}\, m)$, ou seja, $ord(a) \leq r$ se $r > 0$.

Logo, pela definição de *ord(a)*, temos que ter $r = 0$, caso contrário existiria um inteiro $r < ord(a)$ tal que $a^r \equiv 1 (\mathrm{mod}\, m)$.

Portanto $ord(a) \mid k$. □

Como $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, resulta imediatamente da proposição anterior que $ord(a) \mid \varphi(m)$.

Por outro lado, estamos em condições de definir raiz primitiva de um número inteiro.

Definição 8

Seja *a* um número inteiro coprimo com *m*. Se *a* tiver ordem $\varphi(m)$, então *a* denomina-se por raiz primitiva módulo *m*.

Caso o módulo seja um número primo, está garantida a existência de pelo menos uma raiz primitiva, num resultado cuja complexidade extravasa o objetivo deste trabalho.

Entre os muitos contributos que Gauss deu à teoria dos números, alguns dos mais belos e importantes estão associados à noção de resíduo quadrático.

Se o nosso estudo não necessita de aprofundar o tema até momentos tão marcantes da história como a apresentação da lei da reciprocidade quadrática associada à resolução de congruências quadráticas, necessitaremos de outros como o critério de Euler, o símbolo de Legendre e o lema de Gauss.

Definição 9

Sejam *a* e m números inteiros. Então *a* é resíduo quadrático módulo *m* se existir um inteiro *b* tal que $b^2 \equiv a(\mathrm{mod}\, m)$.

Proposição 4 ("Critério de Euler")

Seja *p* um número primo ímpar e *a* inteiro tal que $p \nmid a$. Então *a* é resíduo quadrático módulo *p* se e só se $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$.

Demonstração

Se *a* for resíduo quadrático módulo *p*, então existe um inteiro *b* tal que $b^2 \equiv a(\mathrm{mod}\ p)$. Então temos

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

Como $p \nmid b$, pelo Pequeno Teorema de Fermat temos que $b^{p-1} \equiv 1(\mathrm{mod}\ p)$, ou seja, $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$.

Reciprocamente, suponhamos que $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$.

Seja *r* uma raiz primitiva módulo *p* e $a \equiv r^k (\text{mod } p)$. Deste modo temos

$$1 \equiv a^{\frac{p-1}{2}} \equiv \left(r^k\right)^{\frac{p-1}{2}} = r^{\frac{k(p-1)}{2}} (\text{mod } p).$$

Como *r* é raiz primitiva módulo *p*, temos que $p-1 = ord(r)$. Por outro lado, $r^{\frac{k(p-1)}{2}} \equiv 1 (\text{mod } p)$, ou seja, $p-1 | \frac{k(p-1)}{2}$.

Se $p-1 | \frac{k(p-1)}{2}$, então $\frac{k(p-1)}{2(p-1)} \in \mathbb{Z}$ o que obriga a que $\frac{k}{2} \in \mathbb{Z}$ donde resulta que *k* é número par. Deste modo concluímos que o índice de *a* é par e logo *a* é resíduo quadrático módulo *p*. □

O estudo de Euler dos resíduos quadráticos foi aprofundado pelo matemático francês Adrien Legendre (1752-1833). Deixou publicados muitos resultados importantes associados aos resíduos quadráticos e as suas aplicações.

Em algumas dos resultados que apresentaremos, o recurso ao símbolo de Legendre e algumas das suas propriedades será precioso.

Definição 10 ("Símbolo de Legendre")

Seja *p* primo ímpar e *a* inteiro tal que $p \nmid a$. Definimos

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ se } a \text{ for resíduo quadrático mod p} \\ -1 \quad \text{caso contrário} \end{cases}.$$

Propriedade 6

Seja p um número primo ímpar e a e b dois números inteiros tais que $p \nmid ab$. Se $a \equiv b(\text{mod } p)$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Demonstração

Se a for resíduo quadrático módulo p, então $a \equiv k^2(\text{mod } p)$. Como $a \equiv b(\text{mod } p)$ temos que $b \equiv a \equiv k^2(\text{mod } p)$, donde b também é resíduo quadrático, ou seja, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. □

Propriedade 7

Seja p um número primo ímpar e a e b dois números inteiros tais que $p \nmid ab$. Então $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(\text{mod } p)$.

Demonstração

Como p primo e $p \nmid ab$, temos que $p \nmid a$, ou seja $a^{p-1} \equiv 1(\text{mod } p)$ [2].

Então $1 \equiv a^{p-1} = \left(a^{\frac{p-1}{2}}\right)^2 (\text{mod } p) \Leftrightarrow \left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0(\text{mod } p)$. Temos então que $a^{\frac{p-1}{2}}$ é raiz de $x^2 - 1 \equiv 0 \Leftrightarrow (x-1)(x+1) \equiv 0(\text{mod } p) \Leftrightarrow p \mid (x-1)(x+1)$.

Como p é primo, temos que $p \mid (x-1)$ ou $p \mid (x+1)$, ou seja, $x \equiv 1(\text{mod } p)$ ou $x \equiv -1(\text{mod } p)$.

[2] *Corolário 1*

Deste modo, se *a* for resíduo quadrático, $a \equiv k^2 (\text{mod } p) \Leftrightarrow a^{\frac{p-1}{2}} \equiv \left(k^2\right)^{\frac{p-1}{2}} = k^{p-1} \equiv 1(\text{mod } p)$ visto que se *p* primo, $p \nmid a$ e $a \equiv k^2 = k \cdot k$, então $p \nmid k$.

Concluímos assim que se $a^{\frac{p-1}{2}}$ resíduo quadrático então $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, caso contrário, $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, ou seja, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(\text{mod } p)$. □

Propriedade 8

Seja *p* um número primo ímpar e *a* e *b* dois números inteiros tais que $p \nmid ab$. Então $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração

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

Para finalizar, apresentaremos um resultado que permitirá determinar rapidamente se 2 é ou não resíduo quadrático módulo *p*.

Sendo um resultado mais técnico e teórico, será posteriormente útil aquando do cálculo do símbolo de Legendre em situações concretas.

Teorema 7 ("Lema de Gauss")

Seja *p* um primo impar e seja *a* um número inteiro tal que $p \nmid a$. Consideremos o conjunto $S = \left\{ a, 2a, 3a, ..., \left(\frac{p-1}{2} \right) a \right\}$ e seja *n* o número de elementos de *S* cujo resto da divisão inteira por *p* excede $\frac{p}{2}$.

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

Demonstração

Como *p* é primo, $p \nmid b,\ \forall b \in B = \left\{ 1, 2, ..., \frac{p-1}{2} \right\}$.

Consideremos dois elementos quaisquer $b_i a$ e $b_j a$ de $S = \left\{ a, 2a, 3a, ..., \left(\frac{p-1}{2} \right) a \right\}$. Suponhamos que $b_i a \equiv b_j a (\text{mod } p)$. Sem perda de generalidade, suponhamos que $i > j$. Então teríamos $b_i a \equiv b_j a \Leftrightarrow b_i a - b_j a \equiv 0 \Leftrightarrow \left(b_i - b_j \right) a \equiv 0 (\text{mod } p)$. Como $p \nmid a$ e *p* é primo, temos que $p \mid (b_i - b_j)$ o que é absurdo visto a maior diferença possível entre dois elementos *B* ser menor que *p*.

Deste modo concluímos que nenhum dos elementos de *S* é divisível por *p*, nem existem dois elementos de *S* congruentes estre si módulo *p*.

Sejam $r_1, ..., r_m$ os restos da divisão dos elementos de *S* menores que $\frac{p}{2}$ e sejam $s_1, ..., s_n$ os restos da divisão dos elementos de *S* maiores que $\frac{p}{2}$. Temos então que $m + n = \frac{p-1}{2}$ e que $r_1, ..., r_m, p - s_1, ..., p - s_n$ são todos números inteiros positivos menores que $\frac{p}{2}$. Seja $C = \left\{ r_1, ..., r_m, p - s_1, ..., p - s_n \right\}$.

Podemos concluir que todos os elementos de *C* são distintos. Para tal, basta mostrar que $p - s_i \neq r_j, \forall i \in \{1,...,m\}, \forall j \in \{1,...,n\}$. Suponhamos que existem s_i e r_j tais que $p - s_i = r_j \Leftrightarrow p = s_i + r_j$, o que é absurdo pois $s_i, r_j < \frac{p}{2}$.

Então existem inteiros *u* e *v* pertencentes a *B* tais que $s_i \equiv ua \pmod{p}$ e $r_j \equiv va \pmod{p}$. Deste modo temos que

$$ua + va = (u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}.$$

Como $p \nmid a$ e *p* é primo, temos que $p \mid (u+v)$, o que é absurdo pois $u + v \leq p - 1$.

Assim, como todos os elementos de $C = \{r_1,...,r_m, p - s_1,..., p - s_n\}$ são números inteiros positivos distintos e $\#C = n + m = \frac{p-1}{2}$, podemos concluir que $C = B = \left\{1, 2, ..., \frac{p-1}{2}\right\}$ independentemente da ordem pela qual se apresentam os seus elementos.

Ora o produto de todos os elementos de *b* é $\left(\frac{p-1}{2}\right)!$.

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m \cdot (p - s_1) \cdots (p - s_n) \equiv \\ &\equiv r_1 \cdots r_m \cdot (-s_1) \cdots (-s_n) \pmod{p} \equiv \\ &\equiv (-1)^n r_1 \cdots r_m \cdot s_1 \cdots s_n \pmod{p}.\end{aligned}$$

Por outro lado, temos que os números $r_1,...,r_m, s_1,..., s_n$ são congruentes módulo p com algum dos elementos de $S = \left\{a, 2a, 3a, ..., \left(\frac{p-1}{2}\right)a\right\}$, pelo que

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right)a \pmod{p} = \\ &= (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Como *p* é primo, $p \nmid \left(\frac{p-1}{2}\right)!$, ou seja,

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! (\text{mod } p) \Leftrightarrow$$

$$\Leftrightarrow 1 \equiv (-1)^n a^{\frac{p-1}{2}} (\text{mod } p) \Leftrightarrow$$

$$\Leftrightarrow (-1)^n \cdot 1 \equiv (-1)^n \cdot (-1)^n a^{\frac{p-1}{2}} (\text{mod } p) \Leftrightarrow$$

$$\Leftrightarrow a^{\frac{p-1}{2}} \equiv (-1)^n (\text{mod } p).$$

Uma vez que $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$ [3], podemos concluir que $\left(\frac{a}{p}\right) \equiv (-1)^n (\text{mod } p)$. □

Teorema 8

Seja *p* um primo ímpar. Então $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1(\text{mod } 8) \text{ ou } p \equiv 7(\text{mod } 8) \\ -1 & \text{se } p \equiv 3(\text{mod } 8) \text{ ou } p \equiv 5(\text{mod } 8) \end{cases}$.

Demonstração

De acordo com o lema de Gauss, $\left(\frac{2}{p}\right) \equiv (-1)^n (\text{mod } p)$, para *n* igual ao número de elementos do conjunto dos números inteiros $S = \left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, ..., \left(\frac{p-1}{2}\right) \cdot 2\right\} = \{2, 4, 6, ..., p-1\}$ cujo resto da divisão por *p* é superior a $\frac{p}{2}$. Como todos os elementos de *s* são menores que *p*, para determinar *n*, basta contabilizar os elementos de *S* que são maiores que $\frac{p}{2}$.

Para um valor *k* tal que $1 \le k \le \frac{p-1}{2}$, temos que $k < \frac{p}{4} \Leftrightarrow 2k < \frac{p}{2} \le \frac{p-1}{2}$.

[3] *Propriedade 7*

Denotemos por $\left[\frac{p}{4}\right]$ o maior inteiro menor ou igual que $\frac{p}{4}$. Temos então $\left[\frac{p}{4}\right]$ elementos de *S* menores que $\frac{p}{2}$, ou seja, $n=\frac{p-1}{2}-\left[\frac{p}{4}\right]$.

Deste modo temos quatro possibilidades uma vez que um número primo impar é da forma $8k+1$, $8k+3$, $8k+5$ ou $8k+7$, a saber:

se $p=8k+1$, então $n=4k-\left[2k+\frac{1}{4}\right]=4k-2k=2k$;

se $p=8k+3$, então $n=4k+1-\left[2k+\frac{3}{4}\right]=4k+1-2k=2k+1$;

se $p=8k+5$, então $n=4k+2-\left[2k+1+\frac{1}{4}\right]=4k+2-(2k+1)=2k+1$;

se $p=8k+7$, então $n=4k+3-\left[2k+1+\frac{3}{4}\right]=4k+3-(2k+1)=2k+2$.

Assim, se $p=8k+1$ ou $p=8k+7$, temos *n* par donde resulta que $\left(\frac{2}{p}\right)\equiv(-1)^n=1(\text{mod } p)$. Se $p=8k+3$ ou $p=8k+5$, temos n ímpar donde resulta que $\left(\frac{2}{p}\right)\equiv(-1)^n=-1(\text{mod } p)$. □

Deste modo, terminamos o capítulo deste trabalho destinado à apresentação e demonstração dos resultados que servirão de suporte para a exploração dos números primos de Mersenne e dos números perfeitos, principal objetivo desta exploração.

Estes estudos farão com que as análises seguintes sejam mais fluidas.

CAPÍTULO II

II. NÚMEROS PERFEITOS

II.1. EUCLIDES

Número Perfeito

Um número natural diz-se perfeito se for igual à soma de todos os seus divisores positivos com exceção dele próprio, ou seja, se $n = \sigma(n) - n \Leftrightarrow \sigma(n) = 2n$.

Na sua mais famosa obra, os *Elementos*, Euclides não só define número perfeito, como enuncia e demonstra um método para os calcular. Este método ficou conhecido por "fórmula dos números perfeitos euclidianos" que a seguir se demonstra:

Teorema 9

Sendo $n \in \mathbb{N}$, se $2^n - 1$ for número primo, então o número da forma $2^{n-1}(2^n - 1)$ é perfeito.

Demonstração

Sejam $2^n - 1 = p$, número primo e $a = p2^{n-1}$. Pretendemos provar que, nestas condições, *a* é um número perfeito.

Os divisores próprios de *a* são: $1, 2, 2^2, ..., 2^{n-1}, p, 2p, 2^2 p, ..., 2^{n-2} p$.

Então,

$$\sigma(a) = 1 + 2 + 2^2 + \cdots + 2^{n-1} + p + 2p + 2^2 p + \cdots + 2^{n-2} p =$$
$$= \left(1 + 2 + 2^2 + \cdots + 2^{n-1}\right) + p\left(1 + 2 + 2^2 + \cdots + 2^{n-2}\right) =$$
$$= 2^n - 1 + p\left(2^{n-1} - 1\right) = 2^n - 1 + \left(2^n - 1\right)\left(2^{n-1} - 1\right) =$$

$$= \left(1 + \left(2^{n-1} - 1\right)\right)\left(2^n - 1\right) =$$
$$= 2^{n-1}\left(2^n - 1\right) = a$$

Donde se conclui que $\sigma(a) = a$, ou seja, que *a* é número perfeito. □

II.2. NICÓMACO

II.2.1. CONJETURAS

Apesar de não existirem registos físicos que o comprovem, Nicómaco de Gerasa terá vivido no final do séc. I d.C. Segundo os historiadores, foi o primeiro a escrever sobre o pensamento e os ensinamentos matemáticos dos Pitagóricos, cujo auge teve lugar seis séculos antes. Deste modo, as suas obras tornaram-se uma das mais importantes referências deste período.

Num desses manuscritos, *Introdução à Aritmética*, que foi traduzido para latim por Lúcio Apuleio no séc. II e, mais tarde, por Boécio no séc.V, Nicómaco não só define números perfeitos como sendo aqueles cuja soma dos seus divisores próprios[4] é igual ao próprio número, como introduz um sentido filosófico à classificação de "perfeito", como se depreende do seguinte excerto:

[4] *Todos os divisores de um número exceto ele próprio*

> *Como as coisas justas e excelentes são muito poucas e facilmente enumeráveis, enquanto as coisas feias e demoníacas abundam, também os números deficientes*[5] *e superabundantes*[6] *existem numa enorme quantidade e de uma forma irregular, e os números perfeitos são facilmente enumeráveis e aparecem numa determinada ordem, pois:*
>
> *- só existe um entre as unidades (6),*
>
> *- um só entre as dezenas (28) e*
>
> *- um terceiro entre as centenas (496) e*
>
> *- um quarto entre os limites dos milhares (8128).*
>
> *E a sua característica constante é acabar alternadamente entre 6 e 8 e serem sempre pares.*

Nicómaco não só conjetura sobre algumas propriedades dos números perfeitos, como consubstancia essas afirmações mencionando um método, que diz já existir (provavelmente tendo por base o trabalho do pitagóricos ou de Euclides), que permite obter números perfeitos:

> *A partir das potências de 2 e iniciando na unidade*[7]*, vamos somando desde o primeiro até encontrarmos um número primo; então multiplicamo-lo pela última parcela da soma efetuada, obtendo assim um número perfeito.*

Este procedimento corresponde à proposição IX, 36 dos *Elementos* de Euclides abordada no ponto anterior[8].

[5] *Números deficientes - a soma dos divisores próprios é menor que o próprio número*
[6] *Números superabundantes - a soma dos divisores próprios excede o próprio número*
[7] *1 não era considerado potência de 2*
[8] *Teorema 9*

II.2.2. ANÁLISE DAS CONJETURAS

Atualmente sabemos que a distribuição dos números perfeitos não verifica todas as conjeturas de Nicómaco.

Sendo verdade que os primeiros números perfeitos são 6, 28, 496 e 8128, a suposição de que estes terminam alternadamente em 6 ou 8 não se verifica. Os números perfeitos seguintes são:

quinto – $2^{12}\left(2^{13}-1\right)=33550336$

sexto – $2^{16}\left(2^{17}-1\right)=8589869056$

sétimo – $2^{18}\left(2^{19}-1\right)=137438691328$

oitavo – $2^{30}\left(2^{31}-1\right)=2305843008139952128$

No entanto, podemos afirmar que um número perfeito da forma $2^{n-1}(2^n-1)$ termina em 6 ou em 28.

Teorema 10

Se $N=2^{k-1}(2^k-1)$ é um número perfeito euclidiano então:

i) se $k=2$ então $N=6$;

ii) se $k\equiv 1(\mathrm{mod}\,4)$ então $N\equiv 6(\mathrm{mod}\,10)$;

iii) se $k\equiv 3(\mathrm{mod}\,4)$ então $N\equiv 28(\mathrm{mod}\,100)$

Demonstração

i) se $k=2$ então $N=6$;

Por definição de número perfeito euclidiano, temos que 2^k-1 é primo, ou seja, temos que k tem de ser um número primo[9].

Se $k=2$, resulta de imediato que $N=2^{2-1}(2^2-1)=6$.

Caso contrário, *k* é um primo ímpar, donde[10] $k\equiv 1(\mathrm{mod}\,4)$ ou $k\equiv 3(\mathrm{mod}\,4)$. □

ii) se $k\equiv 1(\mathrm{mod}\,4)$ então $N\equiv 6(\mathrm{mod}\,10)$;

Seja $k\equiv 1(\mathrm{mod}\,4)$, ou seja, $k=4n+1\Leftrightarrow k-1=4n$.

Temos assim que $2^{k-1}=2^{4n}$. Ora, $2^{4n}=\left(2^4\right)^n=16^n\equiv 6^n(\mathrm{mod}\,10)$. Mas $6\equiv 6(\mathrm{mod}\,10)$ e $6^2=36\equiv 6(\mathrm{mod}\,10)$, sendo possível provar por indução que para qualquer *n* natural, $6^n\equiv 6(\mathrm{mod}\,10)$, ou seja,

$$2^{k-1}=2^{4n}=\left(2^4\right)^n=16^n\equiv 6^n\equiv 6(\mathrm{mod}\,10).$$

Por outro lado, $2^k-1=2\cdot 2^{k-1}-1\equiv 2\cdot 6-1=11\equiv 1(\mathrm{mod}\,10)$.

Portanto, se $k\equiv 1(\mathrm{mod}\,4)$, $N=2^{k-1}(2^k-1)\equiv 6\cdot 1=6(\mathrm{mod}\,10)$. □

iii) se $k\equiv 3(\mathrm{mod}\,4)$ então $N\equiv 28(\mathrm{mod}\,100)$

Seja $k\equiv 3(\mathrm{mod}\,4)$, ou seja, $k=4n+3\Leftrightarrow k-1=4n+2$.

Temos assim que $2^{k-1}=2^{4n+2}=2^{4n}\cdot 2^2=4^{2n}\cdot 4\equiv 0(\mathrm{mod}\,4)$, ou seja, que $4\mid 2^{k-1}$. Assim, pelo critério de divisibilidade por quatro[11], 4 divide o número formado pelo dois últimos algarismos de 2^{k-1}.

[9] *Teorema 2*
[10] *Teorema 4*
[11] *Propriedade5*

Por outro lado, $2^{k-1} = 2^{4n+2} = 2^{4n} \cdot 2^2 \equiv 6 \cdot 4 = 24 \equiv 4 (\mathrm{mod}\, 10)$, donde resulta que o algarismo das unidades de 2^{k-1} é 4.

Portanto, $2^{k-1} \equiv 10a + 4 (\mathrm{mod}\, 100)$, para algum algarismo $a \in \mathbb{N}_0$. Como $4 \mid 2^{k-1}$, temos que $4 \mid (10a + 4)$, ou seja, como $4 \mid 4$ temos que $4 \mid 10a$ donde resulta de imediato que $a \in \{0, 2, 4, 6, 8\}$.

Assim, $2^{k-1} \equiv 4,\ 24,\ 44,\ 64$ ou $84 (\mathrm{mod}\, 100)$.

Como $2^k - 1 = 2 \cdot 2^{k-1} - 1$, temos que

$2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 4 - 1 = 7 (\mathrm{mod}\, 100)$ ou

$2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 24 - 1 = 47 (\mathrm{mod}\, 100)$ ou

$2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 44 - 1 = 87 (\mathrm{mod}\, 100)$ ou

$2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 64 - 1 = 127 \equiv 27 (\mathrm{mod}\, 100)$ ou

$2 \cdot 2^{k-1} - 1 \equiv 2 \cdot 84 - 1 = 167 \equiv 67 (\mathrm{mod}\, 100)$.

Assim, $2^k - 1 \equiv 7,\ 47,\ 87,\ 27$ ou $67 (\mathrm{mod}\, 100)$.

Consequentemente,

$N = 2^{k-1}(2^k - 1) \equiv 4 \cdot 7,\ 24 \cdot 47,\ 44 \cdot 87,\ 64 \cdot 27$ ou $84 \cdot 67 (\mathrm{mod}\, 100)$, ou seja,

$$N \equiv 28,\ 1128,\ 3828,\ 1728 \text{ ou } 5628 (\mathrm{mod}\, 100).$$

Portanto, $N \equiv 28 (\mathrm{mod}\, 100)$. □

Apesar de algumas conjeturas não terem sido verificadas, Nicómaco lançou os alicerces para a busca e o estudo dos números perfeitos, ajudando a aguçar a curiosidade e o engenho dos matemáticos que lhe sucederam.

II.3. EULER

Leonhard Euler (1707-1783), brilhante matemático suíço, começou por estudar teologia na Universidade de Basileia onde conheceu Johann Bernoulli, na altura um dos mais proeminentes matemáticos europeus. Consequentemente, Euler acabou por abandonar o curso de teologia e dedicou-se exclusivamente ao estudo da matemática, tendo o seu génio cedo sido reconhecido pela Academia de Ciências de Paris que o premiou, tendo este apenas 19 anos.

Entre outros resultados da teoria dos números, Euler demonstrou o reciproco do teorema de Euclides[12], ou seja, que todos os números perfeitos pares são da forma $2^{k-1}(2^k-1)$, onde 2^k-1 é primo.

Teorema 11

Se *n* é um número perfeito par, então $n=2^{k-1}(2^k-1)$, com 2^k-1 número primo.

Demonstração

Seja *n* é um número perfeito par.

Como *n* é par, pode ser escrito da forma $n=2^{k-1}\cdot m$, onde *m* é um número inteiro ímpar e $k\geq 2$.

[12] *Teorema 9*

Temos então que $\sigma(n)=\sigma\left(2^{k-1}\cdot m\right)$. Como σ é multiplicativa[13], resulta que $\sigma(n)=\sigma\left(2^{k-1}\cdot m\right)=\sigma\left(2^{k-1}\right)\sigma(m)$.

Por outro lado, sabemos[14] que $\sigma\left(2^{k-1}\right)=\dfrac{2^{k-1+1}-1}{2-1}=2^k-1$.

Assim, $\sigma(n)=\left(2^k-1\right)\sigma(m)$.

Como *n* é número perfeito, temos que $\sigma(n)=2n=2\cdot 2^{k-1}\cdot m=2^k\cdot m$. Portanto, por um lado $\sigma(n)=\left(2^k-1\right)\sigma(m)$, e por outro, $\sigma(n)=2^k\cdot m$, ou seja,

$$2^k\cdot m=\left(2^k-1\right)\sigma(m).$$

Podemos então concluir que $\left(2^k-1\right)\left|\left(2^k\cdot m\right)\right.$.

Como 2^k-1 e 2^k são coprimos, pelo Lema de Euclides, temos que $\left(2^k-1\right)\left|\, m\right.$.

Seja $m=\left(2^k-1\right)M$. Então,

$$\begin{gathered}2^k\cdot m=\left(2^k-1\right)\sigma(m)\Leftrightarrow\\ \Leftrightarrow 2^k\cancel{\left(2^k-1\right)}M=\cancel{\left(2^k-1\right)}\sigma(m)\Leftrightarrow\\ \Leftrightarrow 2^k M=\sigma(m).\end{gathered}$$

Como $m\,|\,m$ e $M\,|\,m$, resulta que

$$2^k M=\sigma(m)\geq m+M=\left(2^k-1\right)M+M=2^k M\ .$$

Portanto, $\sigma(m)=m+M$.

Ora isto significa que *m* só tem dois divisores, donde se conclui que *m* é primo, ou seja, que os seus divisores são *m* e 1, ou seja, $M=1$.

Concluindo, temos que $m=\left(2^k-1\right)M=\left(2^k-1\right)\cdot 1=2^k-1$. Como *m* é primo, resulta de imediato que 2^k-1 é primo. □

[13] *Propriedade 2*
[14] *Propriedade 3*

II.4. MERSENNE

O Padre Marin Mersenne (1588-1648), depois de ter estudado alguns anos num colégio jesuíta, juntou-se à então recentemente criada Ordem Franciscana de Minims, onde acabou por permanecer até ao fim da sua vida.

Mersenne lamentava o facto de não existir na altura uma organização formal onde os estudiosos da época se pudessem encontrar regularmente para trocar e discutir ideias e descobertas. Assim, disponibilizou o seu próprio quarto no convento Minim para que se pudessem encontrar estudiosos da época, dando origem aos primeiros encontros regulares de matemáticos que decorreram continuamente desde 1635 até à morte de Mersenne em 1648.

Apesar de Mersenne não contribuir de modo muito efetivo para algumas das descobertas efetuadas, o seu espirito inquisidor colocava questões e apresentava ao mundo científico.

Tentou contactar todos nomes importantes no domínio do conhecimento através de uma elaborada rede de correspondência através da qual Mersenne transmitia notícias relativas a avanços científicos em troca de mais informações para divulgação. Deste modo, divulgando questões e solicitando contributos, estimulou o desenvolvimento científico, podendo este processo ser comparada às modernas publicações científicas.

Depois da sua morte, foram encontradas cartas de 78 correspondentes espalhados pela Europa, entre os quais Fermat em França, Huygens na Holanda, Pell e Hobbes na Inglaterra e Galileu e Torricelli na Itália.

Pessoalmente, Mersenne estava mais interessado no conceito grego de divisibilidade, tendo trocado correspondência com Fermat questionando-o sobre a possível factorização de alguns números.

Mersenne estava também interessado em descobrir a existência, ou não, de um número perfeito de vinte ou vinte e um algarismos. A questão subjacente a esta questão é averiguar se o número $2^{37}-1$ é primo. Fermat descobriu que os únicos divisores primos de $2^{37}-1$ teriam de ter a forma $74k+1$ e que 223 é um fator primo de $2^{37}-1$. Deste modo Mersenne ficou a saber da não existência de um número perfeito com vinte ou vinte e um algarismos.

II.4.1. PRIMOS DE MERSENNE

Passou a ser tradicional denominar os números primos da forma 2^k-1, por primos de Mersenne, números esses que passaremos a denotar por M_k.

Pelo que vimos nos pontos anteriores, encontrar um primo de Mersenne 2^k-1 resume-se a estudar os casos em que *k* é primo.

Em 1644, Mersenne afirmou, de forma provocatória, que M_p era primo quando *p* tomava os valores 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257, e composto para todos os outros números primos inferiores a 257.

Na época foi consensual que Mersenne não teria testado a veracidade da afirmação, mas a verdade é que também nenhum outro matemático se aventurou a apresentar um fator primo para os números apresentados.

Entre 1460 e 1588, o matemático italiano Pietro Cataldi provou que M_{17} e M_{19} eram de facto números primos.

Em 1772, Euler verificou que M_{31} era na realidade primo, embora os números M_{67}, M_{127} e M_{257} estivessem para lá da sua capacidade. No entanto, tal esforço comprovou a existência do oitavo número perfeito,

$$2^{30}\left(2^{31}-1\right)=2305843008139952128\,.$$

No entanto a afirmação de Mersenne continha incorreções. Em 1883, Pervouchine, e em 1886, Seelhoff, mostraram, em trabalhos independentes, que M_{61} é primo. Posteriormente, Cole, em 1903, descobriu fatores para M_{67}. Também em 1911, Powers provou que M_{89} é primo. Em 1914, Fauquembergue, e em 1917, Powers, mostraram que M_{107} é primo. Finalmente, em 1922, Kraitchik identificou a última incorreção de Mersenne ao mostrar que M_{257} é composto.

Todos os números compostos M_k, para k inferior a 257, encontram-se atualmente fatorizados. O mais complicado, M_{251}, apenas foi fatorizado em 1984 com o recurso a supercomputadores.

Com a chegada da era informática, a busca de primos de Mersenne, e por consequência, de novos números perfeitos, tem sido efetuada com recurso a computadores. Em 1996 foi fundado o projeto GIMPS (Great Internet Mersenne Prime Search), que partilha a busca por milhões de computadores pessoais de todo o mundo. Deste modo foram descobertos mais catorze primos de Mersenne, sendo o maior e mais recente $M_{57885161}$ encontrado em Janeiro de 2013, elevando o número total de primos de Mersenne para 48.

De salientar ainda que os maiores números primos encontrados nos últimos anos têm sido primos de Mersenne.

II.4.2. PROPRIEDADES DOS PRIMOS DE MERSENNE

No estudo dos primos de Mersenne, deparamo-nos com alguns factos que aguçam a nossa curiosidade. Quando consideramos os primeiros quatro primos de Mersenne (nomeadamente p igual a 3, 7, 31 e 127), e os utilizamos como índices para os primos de

Mersenne, obtemos um primo de Mersenne superior. Isto levou a conjetura de que se M_p é primo de Mersenne, M_{M_p} também será, o que provaria a infinidade dos primos de Mersenne.

Em 1953, o supercomputador Alas, mostrou que $M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$ é um número composto.

Ao longo do tempo, foram criados métodos para determinar se alguns tipos de números de Mersenne são primos ou compostos.

Teorema 12

Se p e $q = 2p + 1$ são primos, então, ou $q \mid M_p$ ou $q \mid (M_p + 2)$, mas não ambos.

Demonstração

Pelo Teorema de Euler, sabemos que $2^{q-1} - 1 \equiv 0 (\mathrm{mod}\, q)$.

Fatorizando obtemos,

$$2^{q-1} - 1 = \left(2^{\frac{q-1}{2}} - 1\right)\left(2^{\frac{q-1}{2}} + 1\right) = \left(2^p - 1\right)\left(2^p + 1\right) \equiv 0 (\mathrm{mod}\, q).$$

Ou seja, temos que $M_p\left(M_p + 2\right) \equiv 0 (\mathrm{mod}\, q)$.

Então concluímos[15] que $q \mid M_p$ ou $q \mid (M_p + 2)$. Se tal ocorresse simultaneamente, teríamos que $q \mid 2$, o que é impossível. □

Posteriormente, e nas condições do teorema anterior, foi possível determinar para que valores $q \mid M_p$ e $q \mid (M_p + 2)$.

[15] *Teorema 3*

Teorema 13

Se $q = 2n+1$ é primo, então:

a) $q \mid M_n$ se $q \equiv 1 (\mathrm{mod}\, 8)$ ou $q \equiv 7 (\mathrm{mod}\, 8)$.

b) $q \mid (M_n + 2)$ se $q \equiv 3 (\mathrm{mod}\, 8)$ ou $q \equiv 5 (\mathrm{mod}\, 8)$.

Demonstração

Como $q = 2n+1$, temos que $n = \dfrac{q-1}{2}$.

a) Dizer que $q \mid M_n$ significa que $q \mid (2^n - 1)$, ou seja, que

$$2^n \equiv 1 (\mathrm{mod}\, q) \Leftrightarrow 2^{\frac{q-1}{2}} \equiv 1 (\mathrm{mod}\, q).$$

Ora, pelo símbolo de Legendre, para que $2^n \equiv 1 (\mathrm{mod}\, q)$ temos de ter $\left(\dfrac{2}{q}\right) = 1$. Então concluímos[16] que $q \equiv 1 (\mathrm{mod}\, 8)$ ou $q \equiv 7 (\mathrm{mod}\, 8)$.

b) Dizer que $q \mid (M_n + 2)$ significa que $q \mid (2^n - 1 + 2) \Leftrightarrow q \mid (2^n + 1)$, ou seja, que

$$2^n \equiv -1 (\mathrm{mod}\, q) \Leftrightarrow 2^{\frac{q-1}{2}} \equiv -1 (\mathrm{mod}\, q).$$

Ora, pelo símbolo de Legendre, para que $2^n \equiv -1 (\mathrm{mod}\, q)$ temos de ter $\left(\dfrac{2}{q}\right) = -1$. Então concluímos[17] que $q \equiv 3 (\mathrm{mod}\, 8)$ ou $q \equiv 5 (\mathrm{mod}\, 8)$. □

Corolário 2

Se p e $q = 2p+1$ são ambos primos impares com $p \equiv 3 (\mathrm{mod}\, 4)$, então $q \mid M_p$.

[16] *Teorema 8*

[17] *Teorema 8*

Demonstração

Um primo impar é da forma[18] $4k+1$ ou $4k+3$.

Se $p=4k+3$, então $q=8k+7$, ou seja, $q\equiv 7(\mathrm{mod}\,8)$ donde resulta que $q\,|\,M_p$.

Se $p=4k+1$, então $q=8k+3$, ou seja, $q\equiv 3(\mathrm{mod}\,8)$ donde resulta que $q\,|\,(M_p+2)$ o que significa que $q\nmid M_p$. □

Aprofundando um pouco mais os resultados anteriores, Fermat restringiu ainda mais os possíveis divisores dos primos de Mersenne.

Teorema 14

Se *p* é um primo impar, então qualquer divisor de M_p é da forma $2kp+1$.

Demonstração

Seja *q* um divisor primo de M_p tal que $2^p\equiv 1(\mathrm{mod}\,q)$.

Seja *k* a ordem de 2 módulo *q*. Sabemos então[19] que $k\,|\,p$.

Se $k=1$, teríamos $2\equiv 1(\mathrm{mod}\,q)$, ou seja $1\equiv 0(\mathrm{mod}\,q)$, donde resulta que $q\,|\,1$, o que é impossível.

Assim, como $k\,|\,p$, $k>1$ e *p* é primo, temos que $k=p$.

Pelo teorema de Euler, temos que $2^{q-1}\equiv 1(\mathrm{mod}\,q)$, donde concluímos[20] que $k\,|\,(q-1)$.

Como $k=p$, temos que $p\,|\,(q-1)$, ou seja, $q-1=pt\Leftrightarrow q=pt+1$.

[18] *Teorema 4*

[19] *Proposição 3*

[20] *Proposição 3*

Caso *t* fosse um inteiro impar, teríamos de ter *q* par, o que contradiz a hipótese considerada.

Logo temos de ter $q = 2kp + 1$. □

Teorema 15

Se *p* é um primo ímpar, então qualquer divisor primo *q* de M_p é tal que $q \equiv \pm 1 (\mathrm{mod}\, 8)$.

Demonstração

Seja *q* um divisor primo de M_p tal que $2^p \equiv 1 (\mathrm{mod}\, q)$. Pelo resultado anterior[21] temos que $q = 2kp + 1$, para um certo *k* inteiro.

Pelo critério de Euler, temos $\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 1 (\mathrm{mod}\, q)$, ou seja, que $\left(\frac{2}{q}\right) = 1$.

Deste modo concluímos[22] que $q \equiv \pm 1 (\mathrm{mod}\, 8)$. □

Não obstante todos os resultados conhecidos e toda a tecnologia envolvida na busca e estudo dos primos de Mersenne e dos números perfeitos, questões como a sua infinidade ou a existência de um número perfeito ímpar continuam por provar ou refutar, pelo que os matemáticos de hoje e de amanhã que se debruçam sobre estas questões continuam a ter temas que aguçam a sua curiosidade e estimulam o seu engenho.

[21] *Teorema 14*

[22] *Teorema 8*

CAPÍTULO III

III. ATIVIDADES PARA A SALA DE AULA

III.1. FUNDAMENTAÇÃO

Neste terceiro e último ponto, pretendemos apresentar algumas propostas de atividades de exploração de algumas das regularidades, propriedades e conjeturas analisadas durante este trabalho, que podem ser exploradas pelos alunos do ensino básico e secundário com recurso a diversos tipos de material de suporte, nomeadamente, calculadoras científicas, calculadoras gráficas e computadores.

A procura e descoberta de regularidades não conferem apenas à exploração matemática motivação e engenho. Servem igualmente como processos para cimentar a organização, o rigor, a coerência e a justificação argumentativa dos resultados descobertos.

Deste modo, a teoria dos números apresenta-se como campo de excelência para a criação deste tipo de atividades dada sua natureza concreta e palpável. Permite que todos os alunos, independentemente do seu grau de proficiência matemática, consigam abordar as situações e realizar as suas explorações de acordo com as suas capacidades, potencializando deste modo o desenvolvimento de novas competências.

A necessidade de transmitir essas descobertas aos seus pares de modo a que todos compreendam, serve de estimulo à objetividade, ao rigor e à coerência da informação transmitida, permitindo aos alunos a apreensão de conhecimento e competências significativas.

III.2. TAREFA 1

Número perfeito: Um número inteiro diz-se perfeito se for igual à soma de todos os seus divisores (com exceção do próprio).

Por exemplo, 6 é um número perfeito pois é divisível por 1, 2, 3 e 6 e $6 = 1 + 2 + 3$.

Completa a seguinte tabela:

Número N	Divisores de N	Soma dos divisores menores que N	Número N	Divisores de N	Soma dos divisores menores que N
1			**16**		
2			**17**		
3			**18**		
4			**19**		
5			**20**		
6			**21**		
7			**22**		
8			**23**		
9			**24**		
10			**25**		
11			**26**		
12			**27**		
13			**28**		
14			**29**		
15			**30**		

Quais os números perfeitos menores que 30?

_____

Um número primo pode ser um número perfeito? Justifica.

_____

III.3. TAREFA 2

Divisor próprio: Os divisores próprios de um número são todos os divisores desse número diferentes dele próprio.

Definição: Um número diz-se **abundante** se for menor que a soma dos seus divisores próprios; diz-se **deficiente** se for maior que a soma dos seus divisores próprios; diz-se **perfeito** se for igual à soma dos seus divisores próprios.

1. Constrói uma tabela que te permita classificar os primeiros vinte números naturais como abundantes, deficientes ou perfeitos.

2. Recorrendo à folha de cálculo, encontra o único número perfeito entre 10 e 100.

3. Relativamente à definição apresentada, existe algum tipo de número que seja obrigatoriamente deficiente? Justifica.

III.4. TAREFA 3

1. Completa a tabela 1 com o resultado da potência a^{p-1}.

TABELA 1				
a \ ***p***	**2**	**3**	**5**	**7**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

2. Completa a tabela 2 com o resto da divisão inteira dos valores da tabela 1 por *p*.

TABELA 2				
a \ ***p***	**2**	**3**	**5**	**7**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

3. Analisa os resultados obtidos na tabela 2. O que observas?

III.5. TAREFA 4

1. Utilizando o Crivo de Eratóstenes, encontra os números primos menores que 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2. Determina o resto da divisão inteira dos primos encontrados por 4. O que observas?

3. Generaliza a regularidade identificada no ponto anterior.

BIBLIOGRAFIA E REFERÊNCIAS

BIBLIOGRAFIA E REFERÊNCIAS

[1] Burton, David M. *"Elementary number theory"*, Mc Graw Hill

[2] Burton, David M. *"The History of Mathematics"*, Mc Graw Hill

[3] Katz, Vitor J. *"História da Matemática"*, Fundação Calouste Gulbenkian

[4] Ore, Oystein. *"Number Theory and its Histoty"*, Mc Graw Hill

[5] Universidade Federal do Ceara

http://www.seara.ufc.br/especiais/matematica/numerosperfeitos/numerosperfeitos00.htm

[6] Silva, Diana Paulo Coelho, Dissertação de Mestrado – *"Alguns marcos históricos relativos a um conceito matemático elementar: um estudo sobre proporções"*. Universidade do Minho.

[7] Queiró, João Filipe, *"Teoria dos números"*, Departamento de Matemática da Universidade de Coimbra, 2002/2003.

[8] *http://www.mat.uc.pt/~caldeira/RaizesPrimit.pdf*

[9] *https://en.wikipedia.org/wiki/Largest_known_prime_number*

[10] *https://primes.utm.edu/notes/by_year.html*

[11] *http://www.mersenne.org/*