Criptografia

2016/2017

O Teorema de Euler

(Teorema de Fermat-Euler)

Relatório do seminário apresentado em 05/05/2017

Docente: Isabel Oitavem

Alunos: Francisco Godinho (41611) e Vasco Coelho (41825)

Índice

Introdução e contexto histórico

Para ser possível discutir em detalhe o teorema descrito neste relatório, teremos que mencionar em primeiro lugar o seu autor - *Leonhard Euler (Fig.1)*.

Fig. 1 - Retrato de Euler

Euler nasceu em 15 de abril de 1707 em Basel, na Suíça. Viria a ser conhecido como um dos mais importantes e influentes matemáticos a nível internacional devido às suas inúmeras descobertas em diversos ramos da matemática; desde teoria de números, teoria de grafos, cálculo diferencial e integral, até à trigonometria e geometria. A sua prolífera intervenção e propensão para a matemática influenciou diversos outros ramos científicos como a mecânica, a dinâmica de fluídos, a astronomia, a teoria musical, entre outros. Posto isto, é importante referir que *Euler* é, ainda hoje, o matemático com mais páginas publicadas, totalizando aproximadamente 500 publicações científicas.

Euler viria mais tarde a desenvolver problemas oculares que lhe custariam a visão, tendo ficado cego em 1766. No entanto, este possível obstáculo não afetou a sua capacidade de investigação, e Euler chegou a atingir um rácio de uma publicação científica por semana. Faleceu em 1783, e ainda hoje são aplicados inúmeros conceitos matemáticos definidos por *Euler* no período da sua vivência.

O ponto principal deste seminário e uma das mais influentes obras de *Euler*, conhecido simplesmente como o teorema de *Euler* ou teorema de *Fermat-Euler*, aplicado à teoria de números, surgiu oficialmente em 1763, enquanto *Euler* procurava obter o menor expoente possível para o qual o Pequeno Teorema de Fermat fosse verdadeiro. *Euler* provou ainda o Pequeno Teorema de Fermat, que foi apresentado sem qualquer prova em 1640 por *Pierre de Fermat*.

É importante considerarmos que este teorema, enunciado há cerca de 3 séculos atrás, é hoje utilizado numa das mais importantes técnicas criptográficas, a criptografia de chave pública, e é uma pedra basilar da comunicação segura em informática, na arquitetura do algoritmo RSA e no protocolo de troca de chaves *Diffie-Hellman*.

Conceitos prévios

Antes de enunciar o teorema de *Euler*, necessitamos de compreender três conceitos iniciais: a definição de congruência, o Pequeno Teorema de *Fermat* (que na realidade é um caso especial do teorema de Euler), e o conceito de números co-primos/relativamente primos.

Comecemos pela noção de congruência.

Congruência

O conceito de congruência é utilizado extensivamente na aritmética modular e define-se da seguinte forma,

> *Para um dado $n \in \mathbb{Z}^+$, dois números inteiros a, b são congruentes se o resto da divisão de a por n igualar o resto da divisão de b por n.*

Outra forma de aplicar esta definição é dizer que $a - b$ é divisível por n.

Para representar uma congruência entre a e b, fazemo-lo da seguinte forma,

$$a \equiv b \pmod{n}$$

E podemos ler esta representação como: a e b são congruentes em módulo n.

e.g.

$23 \equiv 9 \pmod{14}$,	resto da divisão de 23 por 14 $=$ resto da divisão de 9 por 14
$37 \equiv 57 \pmod{10}$,	resto da divisão de 37 por 10 $=$ resto da divisão de 57 por 10
$22 \not\equiv 6 \pmod{7}$,	resto da divisão de 22 por 7 $\neq$ resto da divisão de 6 por 7

O Pequeno Teorema de *Fermat*

Relembremos agora o Pequeno Teorema de *Fermat*, apresentado no seminário anterior.

> *Sejam $a, p \in \mathbb{Z}^+$, p primo, e a não divisível por p:*

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

Resumidamente, a elevado a um número primo $p-1$, desde que **não** seja divisível pelo mesmo, é congruente a 1 em módulo de p. Ou seja, o resto da divisão de ambos os termos da congruência por p dará um resto igual a 1.

Este teorema é fundamental para compreender o Teorema de *Euler*, visto que este último foi formulado a partir do Pequeno Teorema de *Fermat*, generalizando-o (esta generalização será descrita nas secções seguintes). É também utilizado extensivamente para testar a primalidade de números inteiros e é um ponto de partida para a criptografia de chave pública.

Números co-primos/relativamente primos

O conceito de números primos não é estranho a ninguém, mas quando nos referimos a números co-primos ou relativamente primos, estamos a descrever exatamente o quê?

Este conceito é refletido no Teorema de *Euler* sendo uma condição essencial na sua enunciação, portanto temos que o compreender primeiro para o poder utilizar.

Enunciemos então a definição,

Sejam $n, m \in \mathbb{Z}$*:*

n *e* m *são co-primos/relativamente primos se* $\mathrm{mdc}(m, n) = 1$

Ou seja, informalmente podemos considerar dois números co-primos se o máximo divisor comum entre ambos for a unidade. Quaisquer pares de números cujo máximo divisor comum entre ambos for superior a 1, **não** são co-primos.

É importante também mencionar que não se exige nenhuma condição sobre n ou sobre m além de terem que ser inteiros positivos, não sendo necessária nenhuma restrição de primalidade sobre os mesmos. Caso ambos sejam números primos, então são também co-primos.

e.g.

Os pares $(25,2)$, $(35,13)$, $(46,21)$ são pares de números co-primos, visto que $\mathrm{mdc} = 1$

(é de notar que no terceiro par, nem 46, nem 21 são números primos)

Já o par $(9,12)$ não é um par de números co-primos, visto que $\mathrm{mdc} = 3$

O Teorema de Euler

Após compreender os três conceitos descritos nas secções anteriores, podemos então enunciar o Teorema de *Euler*,

> *Sejam* $a, n \in \mathbb{Z}^{+}$ *e co-primos, e* $\varphi(n)$ *a função totiente de Euler:*

$$a^{\varphi(n)} \equiv 1 \ (\mathrm{mod}\ n)$$

Podemos, portanto, verificar algumas semelhanças entre o Pequeno Teorema de *Fermat* e o Teorema de *Euler*. Verificamos que foi introduzida a restrição de co-primalidade sobre a e n, que não existia no Pequeno Teorema de *Fermat*, e que foram removidas as restrições de n (anteriormente denominado por p) ser um número primo e de a ser divisível por n.

No entanto, a maior diferença entre ambos os teoremas é a introdução da função $\varphi(n)$ – a função totiente de *Euler* – que é descrita na secção seguinte.

Apesar das diferenças, o Teorema de *Euler* trata-se de uma generalização do Pequeno Teorema de *Fermat*, e como tal, conseguimos chegar ao caso especial que tem como aplicação o Pequeno Teorema de *Fermat* aplicando as restrições necessárias sobre a e n (veremos na secção seguinte como $\varphi(n)$ se aplica neste caso).

Função totiente de *Euler*

A função totiente de *Euler*, ou simplesmente a função totiente, representada por $\varphi(n)$, define-se da seguinte forma,

$$\varphi(n) = \#\{m \in \mathbb{Z}^{+} \mid m \leq n \wedge \mathrm{mdc}(m, n) = 1\}$$

Informalmente, $\varphi(n)$ retorna o número de inteiros positivos menores ou iguais que n e relativamente primos a n.

Propriedades

A função totiente de *Euler* possui duas propriedades fundamentais:

<u>1ª Propriedade: Multiplicatividade</u>

$$\varphi(mn) = \varphi(m) \cdot \varphi(n), \qquad \text{se } \mathrm{mdc}(m, n) = 1$$

Sucintamente, o que esta propriedade define é que resultado da função totiente cujo argumento é um produto de números co-primos, m e n, é igual ao resultado do produto das funções totientes de ambos os números m e n.

Esta propriedade pode ser provada utilizando o Teorema Chinês do Resto que consiste na resolução de sistemas de congruências lineares.

2ª Propriedade: Potências de números primos

Esta propriedade é um pouco mais complexa que a primeira, mas é essencial para determinar a fórmula matemática que permite calcular a função totiente. Baseia-se em inferir a aplicação da função a potências de números primos e é definida da seguinte forma,

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right), \quad k \geq 1$$

Ou seja, quando o argumento da função totiente é a potência de um número primo, sendo o expoente um inteiro positivo ($k \geq 1$), o resultado daí obtido é a diferença do argumento p^k com p^{k-1}. A segunda igualdade, em que metemos p^k em evidência é apenas por questões de simplificação.

Como é que provamos esta propriedade? Comecemos por considerar todos os números inteiros $m \leq p^k$ para os quais $\mathrm{mdc}(m, p^k) \neq 1$. Ao retirarmos esses números do conjunto total de números inferiores ou iguais a p^k, teremos como resultado o conjunto de números $q \leq p^k$ tais que $\mathrm{mdc}(q, p^k) = 1$, i.e. teremos o conjunto de números co-primos a p^k, o que reflete a definição acima ($\varphi(p^k) = p^k - p^{k-1}$).

Sendo p um número primo, a única possibilidade para que $\mathrm{mdc}(m, p^k) \neq 1$, é que p^k seja um múltiplo de p. Os múltiplos de p^k inferiores ou iguais a p^k são $p, 2p, 3p, \dots, p^{k-1}p$, logo existem p^{k-1} múltiplos de p^k tais que sejam inferiores ou iguais a p^k.

Através desta propriedade, podemos também confirmar a equivalência entre o Teorema de Euler e o Pequeno Teorema de *Fermat* quando n é um número primo, visto que se o argumento da função totiente for um número primo p, daí resulta que $\varphi(p^1) = p^1 - p^0 = p - 1$. Desta forma, teríamos o Teorema de *Euler* na seguinte forma,

$$a^{\varphi(p^1)} \equiv 1 \pmod{p} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$$

Obtendo assim a definição do Pequeno Teorema de *Fermat*.

Fórmula do produto de *Euler* e prova matemática

Dada a definição e as propriedades da função totiente de *Euler*, resta entender como se calculam matematicamente os valores de $\varphi(n)$. Para tal, *Euler* determinou o cálculo da função totiente através da fórmula conhecida como a fórmula do produto de *Euler*, que se apresenta a seguir,

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Onde o produtório da fórmula é feito sobre os p números primos distintos que dividem n, i.e. $p|n$.

Podemos agora verificar como é que *Euler* chegou a esta fórmula e consequentemente prová-la matematicamente:

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}\right) && \text{Teorema fundamental da aritmética} \\
&= \varphi\left(p_1^{k_1}\right) \cdot \ldots \cdot \varphi\left(p_1^{k_1}\right) && \text{1ª Propriedade da função totiente} \\
&= p_1^{k_1}\left(1 - \tfrac{1}{p_1}\right) \cdot \ldots \cdot p_r^{k_r}\left(1 - \tfrac{1}{p_r}\right) && \text{2ª Propriedade da função totiente} \\
&= p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) && \\
&= n \cdot \left(1 - \tfrac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \tfrac{1}{p_r}\right) && \text{Teorema fundamental da aritmética (inv.)} \\
&= n \cdot \textstyle\prod_{p|n}\left(1 - \tfrac{1}{p}\right) && \textbf{Fórmula do produto de \textit{Euler}}
\end{aligned}$$

Utilizando o teorema fundamental da aritmética (que diz que qualquer inteiro positivo pode ser fatorizado no produto de números primos) e as propriedades da função totiente, vemos que é possível chegar à fórmula do produto de *Euler*.

Exemplos práticos da função totiente

Para consolidar os conhecimentos relativamente à função de *Euler* podemos ter em conta os seguintes exemplos:

$\varphi(10) = ?$ e $\varphi(7) = ?$

Por aplicação da fórmula do produto de *Euler*, obtemos que,

$$\varphi(10) = 10 \cdot \left(1 - \tfrac{1}{2}\right) \cdot \left(1 - \tfrac{1}{5}\right) = 10 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} = 4$$

i.e. 10 tem 4 números co-primos inferiores a ele próprio $(1,3,7,9)$

$$\varphi(7) = 7 \cdot \left(1 - \frac{1}{7}\right) = 7 \cdot \frac{6}{7} = 6$$

i.e. 7 tem 6 números co-primos inferiores a ele próprio $(1,2,3,4,5,6)$

Podíamos calcular $\varphi(10)$ e $\varphi(7)$ de outra forma; no caso de $\varphi(10)$ podíamos fatorizar 10 no produto de números primos $2^1 \cdot 5^1$ e aplicar a propriedade de multiplicatividade da função totiente ao argumento da função, posteriormente aplicando a segunda propriedade, enquanto que no caso de $\varphi(7)$ pode ser feita uma aplicação direta da segunda propriedade, visto que 7 já é número primo.

$$\varphi(10) = \varphi(2^1 \cdot 5^1) = \varphi(2^1) \cdot \varphi(5^1) = (2^1 - 2^0) \cdot (5^1 - 5^0) = 1 \cdot 4 = 4$$

$$\varphi(7) = \varphi(7^1) = 7^1 - 7^0 = 6$$

Como vemos, a escolha da forma de cálculo é uma questão de preferência, visto que a própria fórmula do produto de *Euler* foi derivada destas propriedades.

Exemplo prático do teorema de *Euler*

Agora que já compreendemos a função totiente, relembremos a enunciação do teorema:

Sejam $a, n \in \mathbb{Z}^+$ e co-primos, e $\varphi(n)$ a função totiente de Euler:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Uma das aplicações principais do Teorema de *Euler* é a capacidade de reduzir potências de números muito elevadas, difíceis de calcular, em poucas iterações. Para demonstrar isto, consideremos o seguinte exemplo:

Qual é o resto da divisão de 29^{202} por 13?

(Temos aqui um caso em que a potência de um determinado número é demasiado elevada para a podermos calcular normalmente. Temos ainda que dividir o resultado por 13 e obter o resto da divisão, o que dificulta ainda mais a nossa tarefa.

Uma boa solução seria usar o Teorema de *Euler*, mas como?)

Comecemos por considerar então um inteiro positivo co-primo a 29.

$13? \quad \mathrm{mdc}(13, 29) = 1 \quad \checkmark$

Podemos então aplicar o Teorema de *Euler* da seguinte forma

$29^{\varphi(13)} \equiv 1 \Rightarrow 29^{12} \equiv 1 \pmod{13}$

(13 é um número primo, logo esta aplicação do Teorema de *Euler* entra também no caso especial do Pequeno Teorema de *Fermat*. É importante ter em conta que poderia não ser este o caso, e o Teorema de *Euler* mantinha-se verdadeiro desde que as restrições de co-primalidade se assegurassem entre a e n.)

Podemos agora rescrever $202 = 12 \times 16 + 10$,

$29^{202} = 29^{12 \times 16 + 10} = (29^{12})^{16} \times 29^{10}$

Por aplicação do teorema temos que,

$(29^{12})^{16} \times 29^{10} \equiv 1^{16} \times 29^{10} \equiv 29^{10} \pmod{13}$

Podemos ainda reduzir $29^{10} \pmod{13}$ com base no módulo em si,

$29^{10} \equiv 3^{10} = 59049 \equiv 3 \pmod{13}$,

∴ O resto da divisão de 29^{202} por 13 é 3.

(De notar que podia ser aplicado novamente o teorema de *Euler* para reduzir 29^{10}. Optou-se por reduzir diretamente com o módulo de 13 por questões de simplificação.)

Portanto, após este exemplo, podemos verificar que um problema aparentemente difícil de calcular se tornou consideravelmente mais simples pela aplicação do Teorema de *Euler*.

Prova matemática

Existem duas formas distintas de provar matematicamente o Teorema de *Euler*: a primeira utilizando o Teorema de *Lagrange*, e a segunda com base na congruência entre conjuntos de números co-primos recorrendo a permutações. Neste seminário, e por consequente neste relatório, apresentamos a segunda, sendo esta a prova direta do teorema e a originalmente definida por *Euler*.

Apresentemos então a prova:

Seja R o conjunto de todos os inteiros positivos $<\ n$ e relativamente primos a n:

$$R \ = \ \{r_1, r_2, \dots, r_{\varphi(n)}\}$$

Seja $a \ \in \ R$:

Para qualquer r_i existe um j tal que $\quad a \cdot r_i \equiv r_j \pmod n$

r_i e a são inteiros relativamente primos a n, $\therefore$ o produto de ambos é também um inteiro relativamente primo a n. Notemos que a é apenas a permutação de r_i.

Podemos notar ainda que se $a \cdot r_i \equiv a \cdot r_j \pmod n$, então $r_i = r_j$

Desta forma, podemos obter R' através da permutação de R por a:

$$R' \ = \ \{a \cdot r_1, a \cdot \ r_2, \dots, a \cdot r_{\varphi(n)}\}$$

Sendo que:

Os elementos de R e os elementos de R' são congruentes. Como vimos anteriormente, R' é apenas uma permutação sobre R.

$$\prod_{i=1}^{\varphi(n)} a\, r_i \ \equiv \ \prod_{i=1}^{\varphi(n)} r_i \ (mod\, n)$$

Podemos colocar o fator de permutação a em evidência.

$$a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i \ \equiv \ \prod_{i=1}^{\varphi(n)} r_i \ (mod\, n)$$

Se cancelarmos os produtórios, visto serem iguais em ambos os termos da congruência, chegamos ao Teorema de *Euler*.

$$a^{\varphi(n)} \ \equiv 1 \ (mod\, n)$$

Damos então por concluída a prova do teorema.

Aplicações do teorema de *Euler*

As duas aplicações principais do Teorema de *Euler* é a redução de números elevados a grandes potências, como vimos no exemplo prático apresentado nas secções anteriores, e na criptografia, nomeadamente, na criptografia de chave pública ou criptografia assimétrica.

Criptografia de chave pública

O Teorema de *Euler* é utilizado extensivamente em protocolos e algoritmos criptográficos que têm por base a criptografia assimétrica. Os dois principais exemplos desta utilização são o algoritmo RSA e o protocolo de troca de chaves *Diffie-Hellman*, onde o Teorema de *Euler* constitui a arquitetura de ambos.

No caso concreto do protocolo *Diffie-Hellman*, a segurança do protocolo reside na seguinte congruência,

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

Onde a, b e p são as variáveis conhecidas/públicas, p um número primo e x uma variável desconhecida (ou privada). A segurança do protocolo é garantida pela assunção que é computacionalmente difícil encontrar x tal que seja possível satisfazer a congruência linear.

No algoritmo RSA, a força criptográfica do algoritmo reside numa variação semelhante,

$$x^e \equiv c \pmod{N}, \qquad N = pq$$

Onde e, c e N são as variáveis conhecidas (ou públicas) desta congruência linear, e p, q e x as desconhecidas, sendo p e q números primos. Aqui, a dificuldade computacional está em computar as raízes de e em módulo N de modo a satisfazer a congruência, e mais importante que isso, em decompor N nos números primos que o geraram.

O que é importante reter aqui, é que é computacionalmente eficiente gerar N a partir de dois números p e q conhecidos, mas descobrir os números p e q que geraram N é bastante exigente e pouco exequível, e a complexidade temporal para satisfazer esta congruência linear torna-se exponencial com o aumento do tamanho da chave utilizada no algoritmo.

Conclusão

Há 254 anos atrás, *Euler* publicaria oficialmente o Teorema de *Euler*, um marco para a área da aritmética modular, que viria a ser utilizada nos dias de hoje na criptografia assimétrica para garantir a segurança de comunicações e de dados no mundo informático, como é o caso do algoritmo RSA e do protocolo de troca de chaves *Diffie-Hellman*, tecnologias que hoje asseguram a confidencialidade e a integridade das nossas interações na internet, transações bancárias, emails, entre outros.

É importante considerar que o facto da criptografia moderna se basear na matemática clássica, como é o caso do Teorema de *Euler*, contribui para a confiança na força criptográfica dos algoritmos baseados na mesma, visto que ao longo de décadas, ou até mesmo séculos, não foi possível (ou pelo menos não foi divulgada) a existência de falhas criptográficas por meio de criptoanálise. Portanto, a maturidade dos fundamentos dos algoritmos criptográficos que utilizamos é sempre um fator que tem de ser ponderado previamente à sua utilização.

O Teorema de *Euler*, apesar de ter alguma complexidade associada no que toca à sua compreensão, é um ponto de entrada essencial para a criptografia de chave pública, sendo que a realização deste seminário contribuiu bastante para a aprendizagem dos estudantes que o realizaram, e esperamos que tenha também contribuído da mesma forma para quem teve a possibilidade de assistir ao mesmo.

Bibliografia

[1] Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. (2008). *An Introduction to Mathematical Cryptography*. Bibliografia da unidade curricular de Criptografia. Retirado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.9999&rep=rep1&type=pdf em 29/04/17.

[2] Wolfram MathWorld. *Fermat's Little Theorem*. Retirado de http://mathworld.wolfram.com/FermatsLittleTheorem.html a 29/04/17.

[3] Zhao, David (2004). *A Proof of Certain Theorems Regarding Prime Numbers*. Tradução de *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio* por Leonhard Euler. Retirado de http://eulerarchive.maa.org//docs/translations/E054tr.pdf a 30/04/17.

[4] Lavrov, Misha (2012). *Euler's Totient Theorem*. Retirado de http://www.math.cmu.edu/~mlavrov/arml/12-13/number-theory-11-11-12.pdf a 01/05/17.

[5] Wikipedia. *Euler's theorem*. Retirado de https://en.wikipedia.org/wiki/Euler%27s_theorem a 01/05/17.

[6] Wikipedia. *Euler's totient function*. Retirado de https://en.wikipedia.org/wiki/Euler%27s_totient_function a 01/05/17.

[7] Weaving, Timothy (2016). *Euler's Theorem and RSA Public Key Cryptography*. Retirado de http://vknight.org/Computing_for_mathematics/Assessment/IndividualCoursework/PastCourseWorks/2015-2016/weaving2015-2016.pdf em 02/05/17.

[8] Biography.com. *Leonhard Euler*. Retirado de http://www.biography.com/people/leonhard-euler-21342391 a 03/05/17.