O pequeno teorema de Fermat

Relatório

Criptografia 2016/2017

Mestrado integrado em Engenharia Informática

Docente Isabel Kahle

Trabalho realizado por:
António Caeiro nº42486

Caparica, 05 de Maio 2017

Índice

Introdução

O trabalho proposto tem como objetivo realizar um seminário sobre o pequeno teorema de Fermat. Para isso foi realizado uma apresentação, discussão e este relatório sobre o teorema.

Primeiramente, pretende-se mostrar quem foi Pierre de Fermat, a sua biografia e as suas contribuições em várias áreas da Matemática.

A seguir irá ser mostrado o teorema com alguns exemplos para facilitar a compreensão. Finalmente iremos provar o teorema e mostrar algumas aplicações práticas.

A motivação do estudo deste teorema tem a ver com as suas aplicações e consequências. Este teorema originou o teorema de Euler, testes de primalidade e calculo de módulo exponencial. Estes são as bases para alguns algoritmos a encriptação de chave pública (o exemplo mais conhecido é o RSA).

Pierre de Fermat

Biografia

Pierre de Fermat nasceu no ano 1601 ou 1607 em Beaumont-de-Lomagne, França e morreu no ano 1665 em Castres, França. Na sua vida profissional foi um bom advogado no parlamento de Toulouse. A matemática foi a sua paixão, apesar de considerar a como um "hobbie" e dar sempre prioridade ao seu trabalho como advogado, fez grandes contribuições em diversas áreas da matemática. Sendo considerando um dos maiores matemáticos do seu tempo.

Imagem 1 - Percurso da vida fermat(1- Beamount ,2-Orleães, 3- Toulouse, 4- Bordeaux, 5- Toulouse, 6- Castres)

Imagem 2- Pierre de Fermat

O seu pai, Dominique Fermat, foi um comerciante de peles bastante rico, que possibilitou os estudos do filho. Fermat tinha também duas irmãs e um irmão mais velho. Este irmão também tinha o mesmo primeiro nome que Fermat (Pierre), infelizmente morreu muito cedo. O facto de terem o nome bastante semelhante é a causa do debate do ano de nascimento de Fermat.

Entre 1623 e 1629 estudo direito e matemática na universidade Orleans, na universidade de Toulouse e em Bordeaux. Segundo as fontes bibliográficas consultadas, não existe uma coerência sobre a ordem dos sítios onde estudou. Mas sabe-se que conseguiu o seu diploma em Direito na universidade de Orleans, e que estudou matemática em Bordeaux.

Em 1630 comprou um escritório de conselheiro no parlamento de Toulouse, este escritório deu-lhe a possibilidade de mudar o nome de Pierre Fermat para Pierre de Fermat. No ano seguinte começou a trabalhar como advogado e oficial de governo. Em 1638 deixou de trabalhar nas câmaras inferiores e passou a trabalhar nas câmaras superiores do parlamento. No ano 1652 foi promovido a juiz supremo que era o cargo mais alto na corte criminal (esta promoção era feita por senioridade e na década de 1650 a praga chegou à região, o próprio Fermat foi erradamente declarado morto em 1653).

Contribuições

Fermat não costumava publicar os seus trabalhos, a maior parte dos seus contributos foram escritos em cartas que trocava com outros matemáticos ou em anotações em livros. Fermat era fluente em seis línguas (francês, latim, occitano, grego clássico, italiano e espanhol), o seu conhecimento em grego ajudou bastante Fermat a estudar a matemática da Grécia antiga. Era também conhecido por como o *"Príncipe dos Amadores",* pois na altura, não existiam matemáticos profissionais e Fermat é considerado um dos melhores matemáticos da sua época.

Em geometria analítica, Fermat descobriu uma forma de encontrar o máximo e mínimo local e calcular tangentes de curvas. Apesar de Descartes ter o crédito por esta descoberta, Fermat já a tinha descoberto antes da publicação de Descartes.

Um jogador profissional de dados pagou a Blaise Pascal para perceber quais as probabilidades de cada jogada. Pascal trocou umas cartas com Fermat e juntos fundaram a teoria da probabilidade.

Em física Fermat criou uma variação de um principio de Euclid que originou o principio de menor ação que diz que a luz viaja entre dois pontos pelo caminho de menor tempo.

A principal área que fermat contribuí-o foi para a teoria de números, ele é considerado o pai da teoria de números moderna. O seu trabalho nesta área é mais conhecido por dois teoremas.

O último teorema de Fermat que foi encontrado pelo filho na margem de um livro que dizia *"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet." "É impossível separar um cubo em dois cubos, ou expoente quatro em duas ou quatro potências, ou em geral, qualquer poder superior ao segundo, em duas potências semelhantes. Eu descobri uma prova verdadeiramente maravilhosa disso, que esta margem é demasiado pequena para a conter"*. Este teorema só foi provado 300 anos depois pelo professor Andrew Wiles. Nas suas cartas Fermat raramente mostrava a prova dos seus teoremas, dizia que gostava de pôr os outros matemáticos a pensar.

O pequeno teorema de Fermat

Este teorema chama-se "pequeno teorema de Fermat" para distinguir do último teorema de Fermat. Chamam-lhe pequeno porque a prova deste teorema é consideravelmente mais pequena que o outro teorema. Este teorema foi pela primeira vez referenciado a 18 de Outubro de 1640, onde ele escreve uma carta para o seu amigo Frénicle de Bessy enunciando o teorema.

Exemplo prático

Tal como no livro da cadeira antes de enunciar o teorema vamos analisar primeiro, o seguinte exemplo prático:

$$
\begin{array}{llllll}
1^1 \equiv 1 & 1^2 \equiv 1 & 1^3 \equiv 1 & 1^4 \equiv 1 & 1^5 \equiv 1 & 1^6 \equiv 1 \\
2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 1 & 2^4 \equiv 2 & 2^5 \equiv 4 & 2^6 \equiv 1 \\
3^1 \equiv 3 & 3^2 \equiv 2 & 3^3 \equiv 6 & 3^4 \equiv 4 & 3^5 \equiv 5 & 3^6 \equiv 1 \\
4^1 \equiv 4 & 4^2 \equiv 2 & 4^3 \equiv 1 & 4^4 \equiv 4 & 4^5 \equiv 2 & 4^6 \equiv 1 \\
5^1 \equiv 5 & 5^2 \equiv 4 & 5^3 \equiv 6 & 5^4 \equiv 2 & 5^5 \equiv 3 & 5^6 \equiv 1 \\
6^1 \equiv 6 & 6^2 \equiv 1 & 6^3 \equiv 6 & 6^4 \equiv 1 & 6^5 \equiv 6 & 6^6 \equiv 1
\end{array}
$$

Imagem 3 - Potências em módulo de 7

Curiosamente podemos verificar que a coluna mais à direita é sempre 1 em módulo de 7, mas e se continuássemos a explorar esta coluna o que aconteceria?

$7^6 \equiv 0 \qquad 8^6 \equiv 1 \qquad 9^6 \equiv 1 \qquad 14^6 \equiv 0 \qquad 15^6 \equiv 1 \qquad 21^6 \equiv 0$

Claramente com este exemplo prático apercebemo-nos do seguinte padrão (considerando que a é um inteiro):

$$
a^6 \equiv \begin{cases} 1 \pmod 7 & \text{if } 7 \nmid a, \\ 0 \pmod 7 & \text{if } 7 \mid a. \end{cases}
$$

O Teorema

Generalizando o exemplo prático acima demonstrado, temos o pequeno teorema de Fermat. Assumindo que p é primo e a é um número inteiro, então temos:

$$a^{p-1} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \nmid a, \\ 0 \pmod{p} & \text{if } p \mid a. \end{cases}$$

Este teorema é bastante útil para a facilmente testar se um número não é primo, no entanto existem os "*fermat* liars" ou pseudoprimos em que para alguns valores que aparentam ser primos apesar de não serem. E existem ainda os números de *"Carmichael"* que segundo o teorema aparentam ser primos apesar de não os serem.

Prova do teorema

Existem várias provas do teorema de Fermat iremos seguir a prova do livro, mas seguindo exemplo prático para facilitar a compreensão do teorema.

Admitindo que $\boldsymbol{p}$ é primo, $\boldsymbol{a}$ é um número inteiro, se $\boldsymbol{p \nmid a}$ é óbvio que para qualquer potência de $\boldsymbol{a}$ é divisível por $\boldsymbol{p}$. Exemplo: $2 \mid 4, então\ 2 \mid 4^2,\quad 2 \mid 4^3\quad 2|4^4$. Logo só nos precisamos de preocupar quando $\boldsymbol{p}$ não divide $\boldsymbol{a}$.

Considerando a seguinte lista de números:

$$\boldsymbol{a}, 2\boldsymbol{a}, 3\boldsymbol{a}, \ldots, (\boldsymbol{p}\text{-}1)\boldsymbol{a} \quad \text{em módulo } \boldsymbol{p}$$

No futuro iremos considerar $\boldsymbol{p}$ = 5 e $\boldsymbol{a}$ = 2 para visualizar os exemplos gerais. Aplicando a lista acima ao nosso exemplo prático teríamos:

$$2, 4, 8, 16 \equiv 2, 4, 3, 1 \bmod 5$$

Nesta lista existem $\boldsymbol{p - 1}$ números (5 -1) e dizemos que são todos diferentes. Para provar que são todos diferentes vamos retirar quaisquer 2 números $\boldsymbol{r}$ e $\boldsymbol{s}$ e vamos supor que $\boldsymbol{r\,.\,a \bmod p}$ e $\boldsymbol{s\,.\,a \bmod p}$ são iguais. Temos então:

$$\boldsymbol{r.a \equiv s.a\ (mod\ p)}\quad \text{logo temos } \boldsymbol{(r-s).a \equiv 0\ (mod\ p)}$$

No nosso exemplo:

$$\boldsymbol{2r \equiv 2s\ (mod\ 5)}\quad \text{logo temos } \boldsymbol{2(r-s) \equiv 0\ (mod\ 5)}$$

Como sabemos que $\boldsymbol{p}$ é primo, podemos dizer que $\boldsymbol{p}$ divide o produto de $\boldsymbol{ab}$ considerando que $\boldsymbol{a}$ e $\boldsymbol{b}$ sejam inteiros. E como estamos a assumir que $\boldsymbol{p}$ não divide $\boldsymbol{a}$ então por exclusão de partes $\boldsymbol{p} \mid (\boldsymbol{r} - \boldsymbol{s})$. Mas tanto $\boldsymbol{r}$ como $\boldsymbol{s}$ estão entre 1 e $\boldsymbol{p} - 1$ (1 e 5 -1), a diferença entre $\boldsymbol{r}$ e $\boldsymbol{s}$ estará sempre entre $-(\boldsymbol{p} - 2)$ e $\boldsymbol{p} - 2$, e neste intervalo só existe um número que é divisível por $\boldsymbol{p}$ esse número é 0, isto prova que $\boldsymbol{r} - \boldsymbol{s} = 0$ logo $\boldsymbol{r} \cdot \boldsymbol{a} = \boldsymbol{s} \cdot \boldsymbol{a}$. Assim provamos que todos os números na lista são diferentes.

Se multiplicarmos todos os números da lista e reduzirmos a módulo $\boldsymbol{p}$ temos:

$$\mathbf{a} \cdot 2\boldsymbol{a} \cdot 3\boldsymbol{a} \cdot \ldots \cdot (\boldsymbol{p} - 1)\boldsymbol{a} \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (\boldsymbol{p} - 1) \bmod p$$

Simplificando, obtemos:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ mod\ p$$

Cortando os fatoriais obtemos o teorema de fermat, provando-o:

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

Exemplo de aplicação prática

Este teorema é muito útil para facilmente computar módulos em p (sendo p um número primo) de expoentes muitos altos.

Exemplo: Sabendo que 53 é primo descubra o resto da divisão inteira de $3^{100000}\ por\ 53$

Aplicando o teorema de Fermat temos:

$$3^{53-1} \equiv 1\ mod\ 53$$

$\frac{100000}{52}$: quociente = 1923, resto = 4

Logo temos

$$(3^{52})^{1923} = 1^{1923} mod\ 53$$

$$3^{99996} = 1\ mod\ 53$$

$$(3^{52})^{1923} = 1^{1923} mod\ 53$$

$$3^{99996} \cdot 3^4 = 3^4\ mo \quad 53$$

$$3^{100000} = 81\ mod\ 53$$

$$3^{100000} = 28\ mod\ 53$$

Como podemos verificar com muita pouca computação facilmente chegamos ao resultado.

Conclusão

Com este trabalho aprendi bastante sobre quem foi Fermat. Foi um dos grandes matemáticos da sua época, apesar de gastar a maior parte do seu tempo no seu emprego e não se puder dedicar totalmente à matemática.

Fermat fez várias contribuições para a área de matemática, na cadeira de Criptografia, o seu pequeno teorema é bastante relevante para o cálculo de módulos em números primos.

Este teorema possibilita algoritmos de encriptação de chave pública como o RSA que sem este teorema, não seriam viáveis pois iriam demorar muito tempo a computar a encriptação e desencriptação.

Bibliografia

- An Introduction to Mathematical Cryptography (livro usado na cadeira)
- http://www-groups.dcs.st-and.ac.uk/history/Biographies/Fermat.html
- https://pt.wikipedia.org/wiki/Pierre_de_Fermat/
- https://en.wikipedia.org/wiki/Pierre_de_Fermat/
- https://prezi.com/vlhaj8y-j0n1/pierre-de-fermat/
- https://www.youtube.com/watch?v=Ij01HGgxnkA
- https://www.youtube.com/watch?v=w0ZQvZLx2KA
- https://www.youtube.com/watch?v=jbiaz_aHHUQ