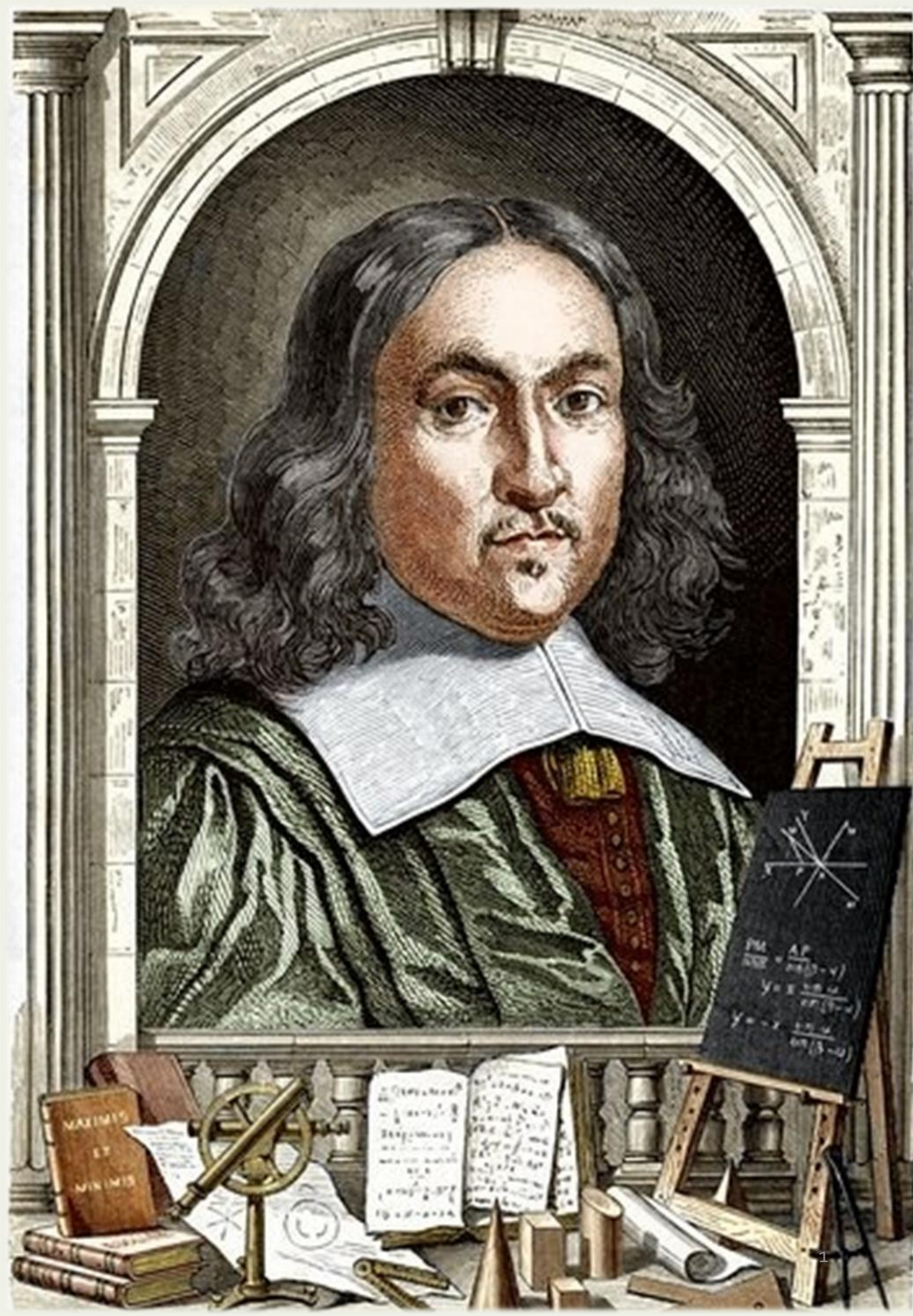


O Pequeno Teorema de Fermat



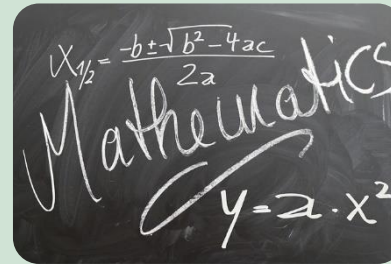
Conteúdo



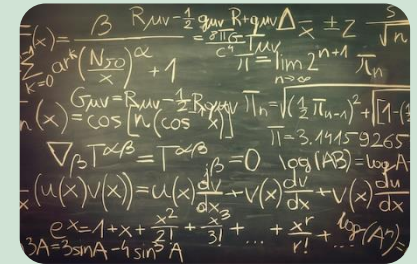
Pierre de
Fermat

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

O Pequeno
Teorema de
Fermat



Exercícios



Aplicações

Pierre de Fermat

Pierre de Fermat nasceu a 17 de Agosto de 1601, em Beaumont-de-Lomagne, França.

Seu pai, Dominique Fermat, era um rico comerciante de peles e segundo cônsul de Beaumont-de-Lomagne.

Vida profissional:

- Câmara inferior do parlamento em 1631;
- Nível mais alto do Tribunal Criminal em 1652.

Pierre de Fermat

Fermat enquanto matemático:

- Várias tentativas falhadas de publicações dos seus trabalhos devido a este não expressar as suas teorias de uma forma polida:
 - Muitos das suas descobertas encontram-se registas em correspondências com outros matemáticos que lhe eram contemporâneos, em textos não publicados e em notas e comentários escritos em livros!!
- Inventa a Geometria Analítica em 1629 e descreve-a num trabalho não publicado: “Introdução aos lugares geométricos planos e sólidos”

Pierre de Fermat



Fermat

VS



Decartes

Pierre de Fermat

Em conclusão:

- Fermat era considerado o “Príncipe dos Amadores”, dedicava-se à Matemática apenas nos seus tempos livres;
- No entanto teve um impacto importantíssimo nesta e foi considerado o melhor matemático do seu tempo por Blaise Pascal.
- Morre em 12 de Janeiro de 1665 em Castre, França, e em 1679 o seu filho junta todas as suas conclusões e publica-as.

Curiosidades:

- Tinha uma vida social reduzida;
- Contribuiu para a Física, ainda que esta área não fosse do seu interesse.

O Pequeno Teorema de Fermat

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

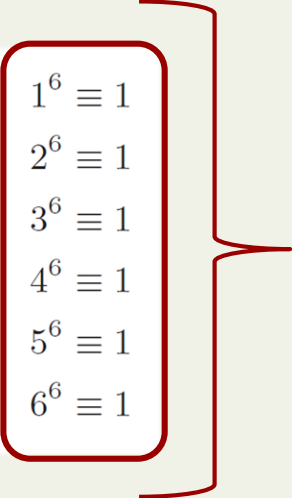

$$a^6 \equiv 1 \pmod{7}, a = 1, \dots, 6$$

Tabela 1: Potências de números módulo 7

Será isto verdade para todos os valores de a ?

O Pequeno Teorema de Fermat

Para:

$$a = 7, 7^6 \equiv 0 \pmod{7}$$

$$a = 14, 14^6 \equiv 0 \pmod{7}$$

$$a = 21, 21^6 \equiv 0 \pmod{7}$$

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

Experiências posteriores com outros primos sugerem que este exemplo reflete um facto geral!

O Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat: Seja p um número primo e a um qualquer número inteiro, então:

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

O Pequeno Teorema de Fermat

Prova:

- $p \mid a \Rightarrow$ é claro que toda a potência de a é divisível por p ;
- $p \nmid a \Rightarrow$

Seja $G = \mathbb{Z}_p^*$ um grupo multiplicativo com um número finito de elementos e H um subgrupo multiplicativo de G , gerado por a .

$$|G| = p - 1$$

$$|H| = h$$

$$H = \{a^0, a^1, \dots, a^{h-1}\}$$

O Pequeno Teorema de Fermat

$$H = \{a^0, a^1, \dots, a^{h-1}\}$$

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

Teorema de Lagrange: se G é um grupo finito e H um subgrupo de G , então a ordem de H divide a ordem de G .

Através do Teorema de Lagrange, podemos dizer que: $|H| \mid |G| \Leftrightarrow h \mid p - 1$, e isto significa que $p - 1 = hm$, para qualquer m . Assim temos que:

$$a^{p-1} \equiv (a^h)^m \pmod{p}$$

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

O Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat: Seja p um número primo e a um qualquer número inteiro, então:

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

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

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

$$p \mid a^{p-1} - 1$$

Exemplo - 1

Sabendo que o número $p = 15485863$ é primo, o Pequeno Teorema de Fermat diz-nos que:

$$2^{15485862} \equiv 1 \pmod{15485863}$$

Assim, sem fazer qualquer computação, sabemos que o número $2^{15485862} - 1$, um número com mais de dois milhões de dígitos, é múltiplo de 15485863!!!

NOTA: normalmente escolhe-se um a no intervalo 2 e $p - 1$, assim sabemos, com certeza que p não divide a .

Exemplo - 2

Qual é o resto de 5^{119} dividido por 59, sabendo que 59 é um número primo?

$$119 = 58 * 2 + 3$$

$$5^{119} = 5^{58*2+3} = (5^{58})^2 * 5^3$$

$$(5^{58})^2 * 5^3 \equiv (1)^2 * 5^3 \equiv 5^3 \equiv 125 \equiv 7 \pmod{59}$$

Novamente, com poucos passos, chega-se a um resultado de forma muito mais eficiente usando o Pequeno Teorema de Fermat.

O Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat: Seja p um número primo e a um qualquer número inteiro, então:

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

⇒ O Teorema diz-nos que quando temos um número primo, aquela condição se verifica... Então, pode ser usado para verificar a primalidade de um número?

Teste de Primalidade

Se queremos testar se um número p é primo, escolhemos um número aleatório a e verificamos se a igualdade se verifica.

- Se não se verificar, sabemos que p não é um número primo;
- Se se verificar, então dizemos que p é um possível primo.

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

Exemplo - 3

Desejamos determinar se $p = 221$ é um número primo.

Vamos escolher $a = 38$:

$$38^{220} \equiv 1 \pmod{221}$$

Assim, ou 221 é um primo, ou 38 é um “Fermat Liar”, vamos experimentar agora para $a = 24$:

$$24^{220} \equiv 81 \pmod{221}$$

Assim, 221 não é um número primo e 38 é um “Fermat Liar”. Mais, 24 é um “Fermat Witness” para o número composto 221.

Aplicações

- O resultado obtido por Fermat é incorporado em algoritmos de forma a reduzir a sua complexidade, tornando-os mais eficientes;
- Testar a primalidade de um número;
- Subjacente nos cálculos utilizados no RSA.

Bibliografia

Burton, David M. (2011), *The History of Mathematics / An Introduction* (7th ed.), McGraw-Hill. p. 511–516. ISBN 978-0-07-338315-6

Hoffstein, Pipher and Silverman (2008), *An introduction to Mathematical Cryptography* (1st ed.), Springer. p. 29–31. ISBN 978-0-387-77993-5

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein (2001). "Section 31.8: Primality testing". *Introduction to Algorithms* (Second ed.). MIT Press; McGraw-Hill. p. 889–890. ISBN 0-262-03293-7.