/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 20 de Abril de 2017

- EQUAÇÕES LINEARES

$3x = 2$

↓ MULTIPLICO OS DOIS LADOS PELO INVERSO MULTIPLICATIVO DE 3

$\left(\frac{1}{3}\right) \cdot 3x = \left(\frac{1}{3}\right) \cdot 2$

$x = \frac{2}{3}$

- CONGRUÊNCIAS LINEARES

$3x \equiv 2 \pmod 7$

↓ MULTIPLICO OS DOIS LADOS PELO INVERSO MULTIPLICATIVO DE 3.

$5 \cdot 3x \equiv 2 \cdot 5 \pmod 7$

$x \equiv 3 \pmod 7$

R	Q	α	β
3	–	1	0
7	–	0	1
3	0	1	0
1	2	-2	1
0	3	–	–

$-2 \equiv 5 \pmod 7$ -> INVERSO

$ax \equiv b \pmod n$

Se a tem inverso multiplicativo módulo n, a congruência tem uma única solução $x \equiv a^{-1} \cdot b \pmod n$

Se a não tem inverso módulo n, a situação é mais complexa. A congruência

pode não ter nenhuma solução ou pode ter várias soluções.

- PEQUENO TEOREMA DE FERMAT:

Seja p um número primo. Seja a um inteiro tal que $a \not\equiv 0 \pmod{p}$ (isto é, p não divide a) então, (**)

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

OBSERVAÇÃO: Não podemos aplicar o teorema de Fermat se o módulo for um número composto!

- SEGUNDA VERSÃO DO TEOREMA:

Seja p um número primo. Então,

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

- DEMONSTRAÇÃO:

Vamos considerar os elementos do conjunto

$$U(p) = \mathbb{Z}_p - \{\bar{0}\}$$
$$= \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$$

→ p-1 ELEMENTOS

MULTIPLICO POR a ($a \not\equiv 0 \pmod p$)

1	$1 \cdot a$
2	$2 \cdot a$
3	$3 \cdot a$
⋮	⋮
j	$j \cdot a$
⋮	⋮
$p-1$	$(p-1) \cdot a$

Se $i \not\equiv j \pmod p$ então,

$i \cdot a \not\equiv j \cdot a \pmod p$.

Suponha, por contradição, que $\underbrace{i \not\equiv j \pmod p}_{(*)}$, mas $ia \equiv ja \pmod p$

$ia \equiv ja \pmod p$

$\Updownarrow$

$ia - ja \equiv 0 \pmod p$

$\Updownarrow$

$(i-j)a \equiv 0 \pmod p$

$\Updownarrow$

p divide $(i-j) \cdot a$

LEMBRANDO: PROPRIEDADE FUNDAMENTAL DOS PRIMOS

Se p divide $a \cdot b$, então p divide a ou p divide b. (só é verdade para primos)

p divide $(i-j) \cdot a$

→ p divide $i-j \Rightarrow i-j \equiv 0 \pmod p \Rightarrow i \equiv j \pmod p \Rightarrow$ CONTRADIZ $(*)$

→ p divide $a \Rightarrow a \equiv 0 \pmod p \Rightarrow$ CONTRADIZ $(**)$

Logo, $ia \not\equiv ja \pmod p$

Logo, como todos os números da lista da esquerda são distintos módulo p, então todos os números da lista da direita também são distintos módulo p.

Assim, ambas as listas contém $p-1$ números distintos módulo p.

Mas, só existem $p-1$ números distintos em $U(p)$. Logo, ambas as listas contém todos os elementos de $U(p)$.

Portanto, o produto dos números na primeira lista vai ser igual (MÓDULO P) ao produto dos números na segunda lista:

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot a \cdot \ldots \cdot (p-1) \cdot a \pmod p$$

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

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

O Teorema de Fermat pode nos auxiliar no cálculo de potências módulo um primo p.

EXEMPLO: $p = 103$

$2^{125\,72683} \pmod{103}$

SEM FERMAT

i	R	A	E	É IMPAR?
	1	2	125 72683	SIM
	2	4	:	

COM FERMAT

$2^{102} \equiv 1 \pmod{103}$

$125\,72683 = 102 \cdot 123261 + 61$

↳ RESTO

↳ QUOCIENTE

$$2^{125\,72683} \equiv 2^{102 \cdot 123261 + 61} \equiv (2^{102})^{123261} \cdot 2^{61}$$

$$\equiv 1 \cdot 2^{61} \pmod{103}$$

R	n	E	É IMPAR?
1	2	64	SIM
2	4	30	NÃO
2	16	15	SIM
32	50	7	SIM
55	28	3	SIM
98	63	1	SIM
97	55	0	NÃO

$2^{125+2683} \equiv 2^{64} \equiv 97 \pmod{103}$

Se quero calcular a^e módulo p, com p primo:

1) Divido e por p-1 (porque $a^{p-1} \equiv 1 \pmod p$)
2) Se r é o resto da divisão, calculo a^r módulo p.

Seja n um número inteiro positivo e a um inteiro tal que $1 < a < n$. Se n for primo, pelo Teorema de Fermat,

$$a^{n-1} \equiv 1 \pmod n.$$

Pensando nisso de forma reversa, se $a^{n-1} \not\equiv 1 \pmod n$, então n é composto.

- TESTE DE FERMAT:

Dado um inteiro n e um inteiro $1 < a < n$, se $a^{n-1} \not\equiv 1 \pmod n$, então n é composto. Neste caso, dizemos que a é uma testemunha que n é composto.

/ /

EXEMPLO: $n = 341$

$a = 3$

TESTE: $3^{340} \equiv 56 \not\equiv 1 \pmod{341}$

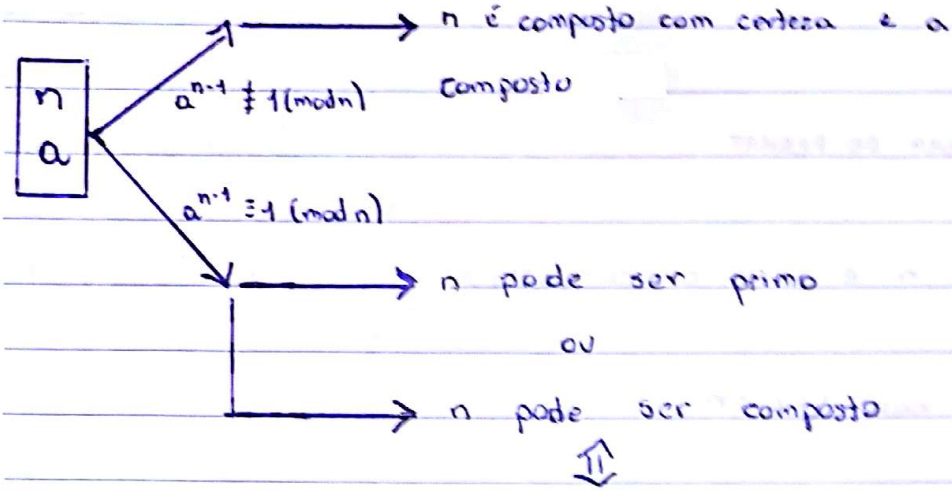
R	A	E	É IMPAR
1	3	340	NÃO
1	9	170	NÃO
1	81	85	SIM
81	82	42	NÃO
81	245	21	SIM
67	9	10	NÃO
67	81	5	SIM
312	82	2	NÃO
312	245	1	SIM
56	9	0	NÃO

PERGUNTA: E se tivéssemos escolhido $a = 2$?

$2^{340} \equiv 1 \pmod{341}$

R	A	E	É IMPAR
1	2	340	NÃO
1	4	170	NÃO
1	16	85	SIM
16	256	42	NÃO
16	64	21	SIM
1	4	10	NÃO
1	16	5	SIM
16	256	2	NÃO
16	64	1	SIM
1	4	0	NÃO

Já sabia que 341 era composto, mas obtive $2^{340} \equiv 1 \pmod{341}$. Logo se $a^{n-1} \equiv 1 \pmod{n}$, não posso concluir nada. n pode ser primo ou n pode ser composto.



341 é um pseudoprimo para a base 2.

Dizemos que n é um pseudoprimo para a base a

DEFINIÇÃO: Se n é composta, mas $a^{n-1} \equiv 1 \pmod{n}$, então n é um pseudoprimo para a base a.

Fixado um a, existem mais primos (verdadeiros) do que pseudoprimos para a base a.

EXEMPLOS DE 1 ATÉ 10^9

↳ 50847534 PRIMOS

↳ 5597 PSEUDOPRIMOS PARA A BASE 2

↳ 1272 PSEUDOPRIMOS PARA AS BASES 2 E 3.

CONCLUSÃO: O Teste de Fermat tem duas respostas possíveis.

↳ COMPOSTO (CERTEZA)

↳ INCONCLUSIVO (PODE SER PRIMO OU COMPOSTO)