UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 25 de Maio de 2017

- EXEMPLOS DE APLICAÇÃO DO ALGORITMO DE GAUSS

1) U(41)

p = 41

p - 1 = 40

Preciso de a_1 tal que $a_1^{(p-1)/2} \not\equiv 1 \pmod{41}$

Preciso de a_2 tal que $a_2^{(p-1)/5} \not\equiv 1 \pmod{41}$

$a_1 = 2$? NÃO!

$2^{40/2} \equiv 2^{20} \equiv 1 \pmod{41}$

$a_1 = 3$? SIM!

$3^{40/2} \equiv 3^{20} \not\equiv 1 \equiv 40 \pmod{41}$

R	A	E	IMPAR
1	2	20	NÃO
1	4	10	NÃO
1	16	5	SIM
16	10	2	NÃO
16	18	1	SIM
1	·	0	NÃO

R	A	E	IMPAR
1	3	20	NÃO
1	9	10	NÃO
1	40	5	SIM
40	1	2	NÃO
40	1	1	SIM
40	1	0	NÃO

$a_2 = 2$? SIM!

$2^{40/5} \equiv 2^8 \equiv 10 \not\equiv 1 \pmod{41}$

R	A	E	IMPAR
1	2	8	NÃO
1	4	4	NÃO
1	16	2	NÃO
1	10	1	SIM
10	18	0	NÃO

$h_1 \equiv a_1^{(p-1)/2^3} \equiv 3^{40/8} \equiv 3^5 \equiv 38 \pmod{41}$

R	A	E	IMPAR
1	3	5	SIM
3	9	2	NÃO
3	40	1	SIM
38	1	0	NÃO

$h_2 \equiv a_2^{(p-1)/5} \equiv 2^{40/5} \equiv 2^8 \equiv 10 \pmod{41}$

$h_1 \cdot h_2 \equiv 38 \cdot 10 \equiv 11 \pmod{41}$

$3 = 11$ ← GERADOR

$U(41) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$

$\phi(40) = \phi(2^3 \cdot 5) = \phi(2^3) \cdot \phi(5) = 2^2 \cdot (2-1) \cdot (5-1) = 4 \cdot 4 = 16$

TODOS OS GERADORES: $11^1, 11^3, 11^7, \ldots \pmod{41}$

2) U(19)

$p = 19$

$p - 1 = 18 = 2 \cdot 3^2$

$a_1^{(p-1)/2} \not\equiv 1 \pmod{19}$

$a_2^{(p-1)/3} \not\equiv 1 \pmod{19}$

$a_1 = 2$? SIM!

$2^{18/2} \equiv 2^9 \equiv 18 \not\equiv 1 \pmod{19}$

R	A	E	IMPAR
1	2	9	SIM
2	4	4	NÃO
2	16	2	NÃO
2	9	1	SIM
18		0	NÃO

/ /

$a_2 = 2$? SIM!

$2^{18/3} \equiv 2^6 \equiv 7 \not\equiv 1 \pmod{19}$

R	A	E	IMPOR
-1	2	6	NÃO
1	4	3	SIM
4	16	1	SIM
7	9	0	NÃO

$h_1 \equiv a_1^{(p-1)/2} \equiv 2^{18/2} \equiv 2^9 \equiv 18 \pmod{19}$

$h_2 \equiv a_2^{(p-1)/3^2} \equiv 2^{18/9} \equiv 2^2 \equiv 4 \pmod{19}$

$h_1 \cdot h_2 \equiv 18 \cdot 4 \equiv 72 \equiv 15 \pmod{19}$

$g = 15$ É GERADOR

TODOS OS GERADORES:

$U(18) = \{1, 5, 7, 11, 13, 17\}$

$15^1, 15^5, 15^7, \ldots \pmod{19}$

- TESTE DE ZUCAS

Já vimos anteriormente que $\phi(n) \leq n-1$ e que $\phi(n) = n-1$ se e somente se n é primo.

Ao invés de testarmos a primalidade diretamente, vamos testar se $\phi(n) = n-1$ ou não.

/ /

Por sua vez, para testar se $\phi(n) = n-1$, buscamos em $U(n)$ se existe ou não um elemento b de ordem $n-1$. Se a ordem de b é $n-1$, então as potências de b geram o subgrupo cíclico de ordem $n-1$. Mas se $U(n)$ contém um subgrupo de ordem $n-1$, então $\phi(n) \geq n-1$.

$\left.\begin{array}{l} \phi(n) \leq n-1 \\ \\ \phi(n) \geq n-1 \end{array}\right\} \phi(n) = n-1$

TESTE DE LUCAS: Seja $n \geq 3$ um inteiro positivo. Então, n é primo se e somente se existe um inteiro b no intervalo $2 \leq b \leq n-1$ que satisfaça as seguintes condições:

(1) $b^{n-1} \equiv 1 \pmod{n}$

(2) $b^{(n-1)/p} \not\equiv 1 \pmod{n}$, para todo fator primo p de $n-1$.

(⇒) Suponha que n é primo. Então, pelo teorema da raiz primitiva, $U(n)$ é cíclico. Logo, existe um elemento g de ordem $(n-1)$ (gerador) em $U(n)$.

Se a ordem de g é $n-1$, então $g^{n-1} \equiv 1 \pmod{n}$ e $g^t \not\equiv 1 \pmod{n}$, para todo $t < n-1$.

Então, em particular, $g^{(n-1)/p} \not\equiv 1 \pmod{n}$ para todo fator primo p de $n-1$.

Logo, as condições (1) e (2) do teste são satisfeitas com $b = g$.

(⇐) Suponha que existe $2 \leq b \leq n-1$ que satisfaça as condições (1) e (2).

Por (1), $b^{n-1} \equiv 1 \pmod{n}$. Então, pelo lema-chave, a ordem de b divide $n-1$. Seja k a ordem de b.

/ /

$n-1 = K \cdot t$

Suponha que $K < n-1$. Então, $t > 1$. Logo, t possui algum fator primo p.

p divide t

t divide n-1

} p divide n-1

$n-1 = K \cdot t$

$\frac{(n-1)}{p} = K \cdot \frac{t}{p}$

↳ INTEIRO (para $\frac{(n-1)}{p}$)

↳ INTEIRO (para $\frac{t}{p}$)

$b^{(n-1)/p} \equiv b^{K(t/p)} \equiv (b^K)^{(t/p)} \equiv 1 \pmod n$

↳ K É A ORDEM

→ CONTRADIÇÃO COM A CONDIÇÃO (2) DO TESTE DE LUCAS

Logo, a ordem de b é n-1.

⇓

$\phi(n) = n-1$

⇓

n é primo

OBSERVAÇÕES: (1) Se para qualquer b, obtivermos $b^{n-1} \not\equiv 1 \pmod n$, podemos encerrar o teste e concluir que n é composto.

(2) Lucas x Miller-Rabin

Vantagem de Lucas: dá certeza se o número é primo ou composto.

Desvantagem: depende de uma fatoração (de n-1), enquanto Miller-Rabin não depende de fatoração nenhuma.

/ /

EXEMPLO: $n = 101$

$n-1 = 100 = 2^2 \cdot 5^2$

$b = 2$

$2^{100} \equiv 1 \pmod{101}$

$2^{100/2} \equiv 2^{50} \equiv 100 \neq 1 \pmod{101}$

$2^{100/5} \equiv 2^{20} \equiv 95 \neq 1 \pmod{101}$

R	A	E	IMPAR
1	2	50	NÃO
1	4	25	SIM
4	16	12	NÃO
4	54	6	NÃO
4	88	3	SIM
49	68	1	SIM
100	79	0	NÃO

CONCLUSÃO: 101 é primo.

R	A	E	IMPAR
1	2	100	NÃO
1	4	50	NÃO
1	16	25	SIM
16	54	12	NÃO
16	88	6	NÃO
16	68	3	SIM
78	79	1	SIM
1	-	0	NÃO

R	A	E	IMPAR
1	2	20	NÃO
1	4	10	NÃO
1	16	5	SIM
16	54	2	NÃO
16	88	1	SIM
95	68	0	NÃO

$n = 113$

$n-1 = 112 = 2^4 \cdot 7$

$b = 2$

$2^{112} \equiv 1 \pmod{113}$

$2^{112/2} \equiv 2^{56} \equiv 1 \pmod{113}$ ERRO! *

$2^{112/7} \equiv 2^{16}$ → NÃO É NECESSÁRIO FAZER

PODE-SE IR DIRETO PARA A PRÓXIMA BASE.

R	A	E	IMPAR
1	2	112	NÃO
1	4	56	NÃO
1	16	28	NÃO
1	30	14	NÃO
1	109	7	SIM
109	16	3	SIM
49	30	1	SIM
1	109	0	NÃO

* CONTA NA PRÓXIMA PÁGINA

/ /

R	A	E	IMPAR
1	2	56	NÃO
1	4	28	NÃO
1	16	14	NÃO
1	30	7	SIM
30	109	3	SIM
106	16	1	SIM
1	30	0	NAO

b = 3

$3^{112} \equiv 1 \pmod{113}$

$3^{56} \equiv 112 \not\equiv 1 \pmod{113}$

$3^{16} \equiv 49 \not\equiv 1 \pmod{113}$

R	A	E	IMPAR
1	3	112	NAO
1	9	56	NAO
1	81	28	NAO
1	7	14	NAO
1	49	7	SIM
49	28	3	SIM
16	106	1	SIM
1	-	0	NAO

R	A	E	IMPAR
1	3	56	NAO
1	9	28	NAO
1	81	14	NAO
1	7	7	SIM
7	49	3	SIM
4	28	1	SIM
112	106	0	NAO

R	A	E	IMPAR
1	3	16	NAO
1	9	8	NAO
1	81	4	NAO
1	7	2	NAO
1	49	1	SIM
49	28	0	NAO

CONCLUSÃO: 113 é primo!

- TESTE DE PÉPIN (APLICAÇÃO DO TESTE DE LUCAS DOS NÚMEROS DE FERMAT)

/ /

$F(k) = 2^{2^k} + 1$

$F(k) - 1 = 2^{2^k}$

↳ ÚNICO FATOR PRIMO É 2.

- TESTE DE LUCAS

$b^{(F(k)-1}$ ≡

$b^{(F(k)-1)/2}$ ≡

- TESTE DE PÉPIN: Para $k \geq 2$, $F(k)$ é primo se e somente se

$5^{(F(k)-1)/2} \not\equiv 1 \pmod{F(k)}$

E

$5^{F(k)-1} \equiv (5^{(F(k)-1)/2})^2 \equiv (-1)^2 \equiv 1 \pmod{F(k)}$

Logo, pelo teste de Lucas, $F(k)$ é primo.

No sentido inverso, precisaríamos mostrar que para um número de Fermat a base 5 sempre funciona. Mas isso, depende de um resultado fora do curso, conhecido como Lei da Reciprocidade Quadrática

Ex: $F(4)$

$F(4) = 2^{2^4} + 1 = 2^{16} + 1 = 65537$

$F(4) - 1 = 65536$

$\frac{F(4)-1}{2} = 32768$

$5^{((F(4)-1)/2)} = 5^{32768} \equiv$

R	A	E	IMPAR
1	5	32768	NÃO
1	25	16384	NÃO
1	625	8192	NÃO
1	62940	4096	NÃO
1	39635	2048	NÃO
1	33457	1024	NÃO
1	64426	512	NÃO
1	54653	256	NÃO

/ /

R	A	C	IMPAR
1	58102	128	NAO
1	31534	64	NAO
1	255	32	NAO
1	65025	16	NAO
1	65533	8	NAO
1	16	4	NAO
1	256	2	NAO
1	65536	1	SIM
65536	-	0	NAO

O Teste de Lucas pode apresentar dificuldade quando são necessárias muitas bases para se chegar ao resultado.

Exemplo: $n = 44$ é primo.

A primeira base que funciona no teste é $b = 7$.

Na próxima AULA, vamos ver uma melhoria no teste que permite testar menos bases para obter o resultado.