Números primos

- Inteiro $p > 1$ é *primo* $\Leftrightarrow$ p é divisível apenas por 1 e por p.
- $2, 3, 5, 7, 11, \ldots$.
- À medida que os números se tornam longos, os primos ficam raros.
- probab{inteiro n primo}$\approx 1/\ln n$. Por exemplo:

n	100	1.000
$\frac{1}{\ln n}$	$1/4.6052 = 0.21715$	$1/\ln 1000 = 1/6.9078 = 0.14476$

n	10.000	100.000
$\frac{1}{\ln n}$	$1/\ln 10000 = 1/9.2103 = 0.10857$	$1/\ln 100000 = 1/11.513 = 0.086859$

Z_n e Z_n^*

- Conjunto de todos os inteiros é $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- Conjunto dos inteiros mod$n$ é Z_n. E.g, $Z_{10} = \{0, 1, \ldots 9\}$.
- Conjunto dos inteiros mod$n$ que são *relativamente primos* a n é chamado Z_n^*.
- E.g.. $Z_{10}^* = \{1, 3, 7, 9\}$.
- Note $0 \notin Z_{10}^*$, pois $mdc(0, 10) = 10$.

- A tabela de multiplicação para Z_{10}^* é:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

- É interessante notar que
  - só os inteiros em Z_{10}^* ocorrem nesta tabela.
  - em cada linha (ou coluna) cada elemento de Z_{10}^* ocorre 1 e 1só vez.

Função Φ de Euler

- $\Phi(n)$ simboliza o número de elementos em Z_n^*, também chamado *ordem* de Z_n^*.
- *E.g.*, $\Phi(10) = 4$, pois $Z_{10}^* = \{1, 3, 7, 9\}$.
- Se p for primo, $\Phi(p) = p - 1$, pois $Z_p^* = \{1, 2, 3, \ldots p - 1\}$. E.g, $\Phi(7) = 7 - 1 = 6$, $Z_7^* = \{1, 2, 3, 4, 5, 6\}$
- Se $n = p^\alpha$ com $\alpha > 0$ e p primo, $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. *E.g.*, $\Phi(3^2) = 3^2 - 3^1 = 6. Z_{3^2}^* = \{1, 2, 4, 5, 7, 8\}$

- Se $n = p \times q$, p e q primos (como no RSA), $\Phi(p \times q) = \Phi(p)\Phi(q) = (p-1)(q-1)$. *E.g.*, $\Phi(10) = \Phi(2 \times 5) = (2-1)(5-1) = 4 = |Z_{10}^*|$
- Fórmula geral: se $n = \prod_{i=1}^{k} p_i^{e_i}$,n então $\Phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1})$, onde os p_i são primos

Gerador ou elemento primitivo de Z_n^*

- Seja $a \in Z_n^*$. A *ordem* de a, $ord(a)$, é o menor inteiro positivo s tal que $a^s = 1 \bmod n$.
- *E.g.*, em Z_7^*, $ord(2) = 6$ pois $2^6 \bmod 7 = 1$. Note: $\Phi(7) = 7 - 1 = 6$
- *E.g.*, se $n = 21$ então $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Observe que $\Phi(21) = \Phi(3)\Phi(7) = 2 \times 6 = 12 = |Z_{21}^*|$. As ordens dos elementos em Z_{21}^* são listadas a seguir:

$a \in Z_{21}^*$	1	2	4	5	8	11	13	16	17	19	20
$ord(a)$	1	6	3	6	2	6	6	2	6	6	2

- Seja $g \in Z_n^*, g > 1$. Se $ord(g) = \Phi(n)$, então g é *gerador* ou *elemento*

primitivo de Z_n^*. E neste caso diz-se que Z_n^* é *cíclico*. *E.g.*, em $Z_5^* = \{1,2,3,4\}$, 2 é gerador:

$2^0 \bmod 5 = 1$	$2^1 \bmod 5 = 2$	$2^2 \bmod 5 = 4$	$2^3 \bmod 5 = 3$	$2^4 \bmod 5 = 1$	
	$2^5 \bmod 5 = 2$	$2^6 \bmod 5 = 4$	$2^7 \bmod 5 = 3$	$2^8 \bmod 5 = 1$	Note o ciclo

- Z_{21}^* não contém gerador, pois cf. tabela acima, o elemento com maior ordem possui ordem 6. .
- $Z_{10}^* = \{1,3,7,9\}$ possui gerador $g = 3$, $\Phi(10) = 4$

$3^0 \bmod 10 = 1$	$3^1 \bmod 10 = 3$	$3^2 \bmod 10 = 9$	$3^3 \bmod 10 = 7$	$3^4 \bmod 10 = 1$	
	$3^5 \bmod 10 = 3$	$3^6 \bmod 10 = 9$	$3^7 \bmod 10 = 7$	$3^8 \bmod 10 = 1$	Note o ciclo

- $n = 8$ é o menor inteiro para o qual Z_8^* *não* possui gerador (Schroeder).
- Se Z_n^* possui ≥ 1gerador, então existem $\Phi[\Phi(n)]$ geradores de Z_n^*. *E.g.*, em Z_6^* $\Phi[\Phi(6)] = \Phi[\Phi(2)\Phi(3)] = \Phi(2) = 1$ e o único gerador é 5. Veja a seguir:

$a \in Z_6^*$	1	2	3	4	5
$a^{\Phi(6)} = 1 \bmod 6$?		não: $2^2 \bmod 6 = 4$	não: $3^2 \bmod 6 = 3$	não: $4^2 \bmod 6 = 4$	sim: $5^2 \bmod 6 = 1$

- se p é um primo, Z_p^* possui ≥ 1 gerador.

Teorema de Euler

$$\forall a \in Z_n^*, a^{\Phi(n)} = 1 \bmod n$$

- E.g., em $Z_{10}^* = \{1,3,7,9\}$, $\Phi(10) = 4$, $3^4 \bmod 10 = 1$
- Consequência: $a^{\Phi(n)-1} \bmod n$ é a inversa de $a \bmod n$ pois

$$a^{\Phi(n)-1} \times a = 1 \bmod n$$

- E.g., em $Z_{10}^* = \{1,3,7,9\}$, $\Phi(10) = 4$, $a = 3$, $a^{\Phi(n)-1} = 3^{4-1} \bmod 10 = 7$, e $(7 \times 3) \bmod 10 = 1$.

No RSA, o módulo é $k = p \times q$ (onde p e q são dois primos *ímpares* distintos), e

- a chave particular secreta é s tal que $mdc(s, \Phi(k)) = 1$
- temos que calcular a chave pública u, inversa de $s \bmod \Phi(k)$ que é
  - $s^{\Phi[\Phi(k)]-1} \bmod \Phi(k) = s^{\Phi[(p-1)(q-1)]-1} \bmod \Phi(k) = u$ (a chave pública)
  - pois $s \times u = s \times s^{\Phi[\Phi(k)]-1} = 1 \bmod \Phi(k)$ pelo T. de Euler
- Algoritmo de Euclides estendido para calcular u é mais rápido.

RSA	
chave pública	$k, u = s^{\Phi[\Phi(k)]-1} \bmod \Phi(k)$
chave particular	s

Exemplo do RSA ($p = 5, q = 11, \Phi(5 \times 11) = 40, \Phi(40) = \Phi(2^3 \times 5) = (2^3 - 2^2) \times (5 - 1) = 16$)	
chave pública	$k = 15, u = s^{\Phi[\Phi(k)]-1} \bmod \Phi(N) = 17^{16-1} \bmod 40 = 33$
chave particular	$s = 17$

Problema RSA	
dados	$k, u, y = x^u \bmod n$
calcular	x

Exemplo do Problema RSA	
dados	$k = 40, u = 33, y = 15^{33} \bmod 55 = 20$
calcular	$x = 15$

Note: o cálculo de x é $y^{17} \bmod 55 = 20^{17} \bmod 55 = 15$

As raízes quadradas mod n

- Se n é produto de dois primos p, q como no RSA, um elemento a de Z_n possui raiz quadrada ou não.
- E.g., para $n = 15$ tem-se a tabela a seguir:

$x = \sqrt{a} \bmod n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$x^2 = a \bmod 15$	1	4	9	1	10	6	4	4	6	10	1	9	4	1

- Note: 1 possui 4 raízes quadradas: $1, 4, 11, 14$; $11 = n - 4$, $14 = n - 1$, ou seja, uma raiz é complemento da outra em relação a n, tendo-se dois pares de raízes: $(1, 14)$ e $(4, 11)$
- 4 também possui 4 raízes quadradas: $2, 7, 8, 13$ que são complementares 2 a 2
- $2, 3, 5, 7, 8, 11, 12, 13, 14$ não possuem raízes quadradas $\bmod 15$

Quanto ao número de raízes quadradas, tem-se:

- Se $p > 2$ é um primo e a possui raiz quadrada, então a possui exatamente duas raízes quadradas $\bmod p$. E.g., $\sqrt{3} \bmod 11 = 5$ e 6. Note que $5 = p - 6 = -6 \bmod 11$
- Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ onde os $p_j > 2$ são primos distintos e cada $\alpha_j > 0$, e se a possui raiz quadrada, então a possui exatamente 2^k raízes quadradas distintas $\bmod n$.
- E.g.,
  - as duas raízes quadradas de $5 \bmod 41$ são 28 e 13 ($13^2 \bmod 41 = 5$, e

$28^2 \bmod 41 = 5$)

- E as raízes quadradas de $16 \bmod 21 = 3 \times 7$ são: $4, 10, 11$ e 17, conforme a tabela a seguir.

$1^2 \bmod 21 = 1$	$2^2 \bmod 21 = 4$	$3^2 \bmod 21 = 9$	$4^2 \bmod 21 = 16$
$5^2 \bmod 21 = 4$	$6^2 \bmod 21 = 15$	$7^2 \bmod 21 = 7$	$8^2 \bmod 21 = 1$
$9^2 \bmod 21 = 18$	$10^2 \bmod 21 = 16$	$11^2 \bmod 21 = 16$	$12^2 \bmod 21 = 18$
$13^2 \bmod 21 = 1$	$14^2 \bmod 21 = 7$	$15^2 \bmod 21 = 15$	$16^2 \bmod 21 = 4$
$17^2 \bmod 21 = 16$	$18^2 \bmod 21 = 9$	$19^2 \bmod 21 = 4$	$20^2 \bmod 21 = 1$