Números primos

- Inteiro $p > 1$ é *primo* $\Leftrightarrow$ p é divisível apenas por 1 e por p.
- E.g., $2, 3, 5, 7, 11, \ldots$.
- À medida que os números se tornam longos, os primos ficam raros.
- prob{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
$\frac{1}{\ln n}$	$1/\ln 10000 = 1/9.2103 = 0.10857$	$1/\ln 100000 = 1/11.513 = 0.086859$

- Essa probabilidade é corolário do Teorema de Números Primos que diz: se $\pi(x)$ denota o número de primos $\leq x$, então

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Z_n e Z_n^*

- Conjunto de todos os inteiros é Z.
- 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.
- **Teorema** Z_n^* é fechado sob multiplicação mod$n$

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 $Z_p^* = \{1, 2, 3, \ldots p - 1\}$.
- Se $n = p^\alpha$ com $\alpha > 0$ e p primo, $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. *E.g.*, $\Phi(3^2) = 3^2 - 3^1 = 6$.
- 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.*, $\Phi(2 \times 5) = (2 - 1)(5 - 1) = 4$
- Se $m = \prod_{i=1}^{k} p_i^{e_i}$, então $\Phi(m) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1})$
- Se $n > 1$ for composto, $\Phi(n) \leq n - 2$ (Wagstaff)

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_5^*, $ord(2) = 4$ pois $2^4 \bmod 5 = 1$.
- Pode-se provar que se $a^r = 1 \bmod n$ então $s|r$ onde $s = ord(a)$. Em particular, s divide $\Phi(n)$ (veja o Teorema de Euler adiante).
- *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^*, 2 é gerador:

$$2^1 \bmod 5 = 2, 2^2 \bmod 5 = 4, 2^3 \bmod 5 = 3, 2^4 \bmod 5 = 1.$$

- Z_{21}^* não contém gerador.
- $n = 8$ é o menor inteiro para o qual Z_8^* não possui gerador (Schroeder).

- Se Z_n^* possui gerador, 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 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: $5^2 \bmod 6 = 1$

- A seguir um resumo sobre geradores de Z_n^*:
  - $\{Z_n^*$ possui ≥ 1 gerador$\} \Leftrightarrow \{n = 2, 4, p^k$ ou $2p^k\}$, onde p é um primo ímpar e $k \geq 1$.
  - Em particular, se p é um primo, Z_p^* possui ≥ 1 gerador.
  - Se $g \in Z_n^*$ é um gerador, $g^j \bmod n$ também é um gerador de Z_n^* $\Leftrightarrow mdc(j, \Phi(n)) = 1$.
    - *E.g.*, Z_{14}^* possui um gerador: $g = 3$.
    - $\Phi(14) = \Phi(2)\Phi(7) = 6$, e
    - $3^5 \bmod 14 = 243 \bmod 14 = 5$, $3^6 \bmod 14 = 1$.
    - $mdc(5, \Phi(14)) = 1$ e
    - 5 é gerador: $5^6 \bmod 14 = 1$.
  - $g \in Z_n^*$ é um gerador $\Leftrightarrow g^{\Phi(n)/p} \neq 1 \bmod n$ para cada primo p divisor de $\Phi(n)$.

- *E.g.*, Z_{14}^{*} possui gerador: $g = 3$
- $\Phi(14) = 6$
- Os primos divisores de 6 são: $2, 3$
- $3^{6/2} \bmod 14 = 13$ e $3^{6/3} \bmod 14 = 9$

Teorema de Euler

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

Consequência: $a^{\Phi(n)-1} \bmod n$ é a inversa de $a \bmod n$ pois

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

No RSA, o módulo é $m = p \times q$ (onde p e q são dois primos *ímpares* distintos), e temos que calcular a inversa da chave secreta $s \bmod \Phi(m)$ que é
$s^{\Phi(\Phi(m))-1} \bmod \Phi(m) = s^{\Phi[(p-1)(q-1)]-1} \bmod \Phi(m)$

Resíduo quadrático mod n

- Seja $a \in Z_n^*$. a é um *resíduo quadrático* módulo n (ou um *quadrado* mod n) se existir um $x \in Z_n^*$ tal que $x^2 = a \bmod n$.
- Se tal x não existir, diz-se que a é um *não-resíduo quadrático* mod n.
- O conjunto de todos os resíduos quadráticos mod n é Q_n, e os não-resíduos quadráticos é $\overline{Q}_n$. Observe que como $0 \notin Z_n^*$, $0 \notin Q_n, 0 \notin \overline{Q}_n$
- Seja $g \in Z_p^*$ um gerador de Z_p^* no caso particular de $p > 2$ ser um primo. Neste caso, $a \in Z_p^*$ é um resíduo quadrático $\Leftrightarrow a = g^i \bmod p$ para um i inteiro *par*. Portanto, $|Q_p| = (p-1)/2$ e $|\overline{Q}_p| = (p-1)/2$.
- Por exemplo sendo $g = 2$ um gerador de Z_{11}^*, tem-se:

i	0	1	2	3	4	5	6	7	8	9
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6

- Portanto, $Q_{11} = \{1,3,4,5,9\}$ e $\overline{Q}_{11} = \{2,6,7,8,10\}$.
- Se $n = p \times q$ onde $p > 2$ e $q > 2$ são dois primos distintos, então $\{a \in Z_n^*$ é um resíduo quadrático mod $n\} \Leftrightarrow \{a \in Q_p$ e $a \in Q_q\}$. Logo, deduz-se que $|Q_n| = |Q_p| \times |Q_q| = (p-1)(q-1)/4$ e $|\overline{Q}_n| = 3(p-1)(q-1)/4$.
- Por exemplo para $n = 3 \times 5 = 15$, $Q_3 = \{1\}$ e $\overline{Q}_3 = \{2\}$, e $Q_5 = \{1,4\}$ e

$\overline{Q}_5 = \{2,3\}$. $Q_{15} = \{1,4\}$. $\overline{Q}_{15} = \{2,7,8,11,13,14\}$. Verifique pela tabela a seguir.

x	1	2	3	4
$x^2 \bmod 3$	1	1	0	$1 = 4 \bmod 3$

x	1	2	3	4	5	6
$x^2 \bmod 5$	1	4	4	1	0	1

- Seja $a \in Q_n$. Se $x \in Z_n^*$ satisfaz $x^2 = a \bmod n$, diz-se que x é *raiz quadrada* de a módulo n. Notação: $\sqrt{a} \bmod n$
- Por exemplo, se $n = 15$ 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; 4 também. $6, 9, 10$ não são resíduos quadráticos $\bmod 15$, pois $\notin Z_{15}^*$.

Quanto ao número de raízes quadradas, tem-se:

- Se $p > 2$ é um primo e $a \in Q_p$, 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 $a \in Q_n$, 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.

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