Teorema de Lagrange
G é subgrupo multiplicativo de ordem n, e $a \in G$. Então $ord(a)|n$
Teorema de Fermat
Seja p primo. $\forall a \in Z_p^* : a^{p-1} = 1 \bmod p$

1. Lemas para cálculo de gerador de Z_p^*

Em geral, este problema é computacionalmente difícil, até onde se conhece. No caso particular em que o primo p é da forma $p = 2q + 1$ onde q é primo, pode-se explorar esta propriedade e elaborar um algoritmo rápido para calcular um gerador de Z_p^*. Para tanto provamos dois lemas auxiliares a seguir.

Lemma 1.1. *Seja $p > 2$ primo, $p = 2q + 1$ onde q é primo. Então $g \in Z_p^*$ é gerador se e somente se $g^q \neq 1$ e $g^2 \neq 1$*

Um exemplo pequeno deste lema: $q = 3, p = 2 * 3 + 1 = 7$, $g = 3$, $3^3 \bmod 7 = 6$, $3^2 \bmod 7 = 2$

i	1	2	3	4	5	6
g^i	3	$3^2 \bmod 7 = 2$	$3^3 \bmod 7 = 6$	$3^4 \bmod 7 = 4$	$3^5 \bmod 7 = 5$	$3^6 \bmod 7 = 1$

demonstração do Lema 1.1

[Caso 1 $\Rightarrow$] Supor por absurdo que:

[Caso 1.1] $g^q = 1 \Rightarrow ord(g) = q$, o que contradiz g ser gerador (ou seja, $ord(g) = p-1$)

[Caso 1.2] $g^2 = 1 \Rightarrow ord(g) = 2$, mesma contradição.

[Caso 2 $\Leftarrow$] Queremos provar que $ord(g) = p - 1 = 2q$. Supor por absurdo que existe $r < 2q$ tal que $g^r = 1 \bmod p$

[Caso 2.1] $r = 2 \Rightarrow g^2 = 1$ que contradiz a hipótese

[Caso 2.2] $r \neq 2 \Rightarrow r$ divide $2q$ (pelo T de Lagrange) $\Rightarrow r$ divide q, o que contradiz q ser primo. Q.E.D

Lemma 1.2. *Se $p = 2q + 1$, p, q são primos, g é gerador de Z_p^* e k não é divisível por q ou por 2, então g^k é um gerador de Z_p^**

demonstração do Lema 1.2

[Caso 1] [k não é divisível por q] $g^{kq} = g^{q+(k-1)q} = g^q(\underbrace{g^{2q}}_{=1 \text{ T. Fermat}})^{(k-1)/2} = g^q \times 1 = g^q$.

Como $q < p$ e g não é gerador de Z_q^*, $g^q \neq 1$. E então pelo Lema 1, como $(g^k)^q = g^q \neq 1$, g^k é um gerador de Z_p^*.

[Caso 2] [k não é divisível por 2] Seja $k = jq + r$, resto $r < q$. $g^{2k} = g^{2r}g^{2jq} = g^{2r}(g^{2q})^j = g^{2r} \times 1 = g^{2r}$ (pelo T. de Fermat). Como g não é gerador de Z_{2r}^* e $2r < 2q(= p-1)$ (pois $r < q$), tem-se: $g^{2r} \neq 1$. Então pelo Lema 1, como $(g^k)^2 = g^{2r} \neq 1$, g^k é um gerador de Z_p^*. Q.E.D

Um pequeno contra-exemplo deste lema: $p = 2 * 3 + 1 = 7, q = 3, 3^k = 3^2 \bmod 7 = 2, k = 2$. Pode-se ver que $3^2 \bmod 7 = 2$ não é gerador, apesar de 3 ser gerador.

i	1	2	3	4	5	6
2^i	2	$2^2 \bmod 7 = 4$	$2^3 \bmod 7 = 1$	$2^4 \bmod 7 = 2$	$2^5 \bmod 7 = 4$	$2^6 \bmod 7 = 1$

2. Algoritmo para cálculo de gerador de Z_p^*

Vamor calcular a probabilidade de um g em Z_p^* ser gerador. Ou seja, calcular quantos geradores existem em Z_p^*.
Pelo Lema 1.2, basta calcular inteiro da forma a^k, com k não divisível por 2 ou por q, para $k = 1, 2, 3, ...2q$. Ou seja, a^k para cada k em Z_{2q}^*. Portanto existem $\Phi(2q) = \Phi(2) \times \Phi(q) = q - 1$ geradores ($\Phi()$ é função de Euler).
Vamos elaborar um algoritmo para calcular um gerador neste conjunto.

Algoritmo CalcularGerador
entrada: inteiro primo $p > 2$ tal que $p = 2q + 1$, q primo
saída: um gerador g de Z_p^*
(1) $termina \leftarrow 0$; $q \leftarrow (p-1)/2$; (* $p = 2q + 1$ *)
(2) enqto $termina = 0$ faça {
    (2.1) sortear uniformemente um g em Z_p^*;
    (2.2) se $g^q \neq 1$ e $g^2 \neq 1$ então $\{termina \leftarrow 1;\}$
    } (* fim-enqto *)
(3) devolva (g);

Pelo Lema 1.1, sabemos que g calculado por este algoritmo é um gerador.
A probabilidade deste algoritmo não encontrar um gerador (i.e., insucesso) em *apenas* uma tentativa no laço (2.1) - (2.2) é $\left(\frac{q+1}{2q}\right)$ pois há $q-1$ geradores em Z_{2q} e $2q - (q-1) = q + 1$. E $\left(\frac{q+1}{2q}\right) \approx \frac{1}{2}$ para q suficientemente grande. Portanto, a

probabilidade deste algoritmo não encontrar qualquer gerador em k tentativas é $\left(\frac{1}{2}\right)^k$, que é quase nulo para k suficientemente grande. Por exemplo, para $k = 10$ tentativas esta probabilidade de insucesso do algoritmo é:

$$\left(\frac{1}{2}\right)^{10} = \frac{1}{1024} < 0.001$$