¿Como hallar una raiz primitiva mod p?

1) Elegimos $g_0 \in U(p)$

2) Calcular $|g_0|$

2.1) Si $|g_0| = p-1$ termine

2.2) si $|g_0| < p-1$ encuentro $g_1 : |g_1| > |g_0|$

¿Como encuentro g_1?

a) Calculo $\langle g_0 \rangle$

b) Agarro $h_0 \in U(p)$ y $h_0 \notin \langle g_0 \rangle$

c) Calculo $|h_0|$

c.1) si $|h_0| > |g_0| \Rightarrow g_1 = h$

c.2) si $|h_0| < |g_0| \Rightarrow g_1 = g_0^{|g_0|/a_0} \cdot h_0^{|h_0|/b_0}$

con a_0 y b_0 tales que $mcm(|g_0|, |h_0|) = a_0 \cdot b_0$

y $mcd(a_0, b_0) = 1 : a_0 / |g_0|, \ b_0 / |h_0|$

3) Repito los pasos 1 y 2 con $g_0 = g_1$

Propiedades del Practico

1) $o(g^n) = \frac{o(g)}{mcd(o(g), n)}$

2)

¿Como hacer los ejercicios de congruencias?

$x^m \equiv y \mod n$

1) Si $x \neq 0 \Rightarrow x \in U(n)$ [si n no es primo usamos el teo Chino del resto]
encontramos una raiz primitiva $g \in U(n)$:
$y = g^z$ y $x = g^t$

2) Igualamos congruencias $(g^t)^m \equiv g^z \mod n$
$\Rightarrow mt \equiv z \mod n-1$ (lema) y resolvemos la cuadratica

3) Si la ecuacion tiene solucion $(mcd(m, n-1) \mid z)$
$\Rightarrow \exists \alpha : t \equiv \alpha \mod n-1$
$\Rightarrow \boxed{x \equiv g^\alpha \mod n}$

4) Reducimos si es necesario la congruencia modulo n

OBS: si es $\log_n y =$

→ si tenemos que resolver $\log_p y \mod n$
Llamamos $x = \log_p y$
y lo elevamos en ambos lados a p
$x^p \equiv y \mod n$
Usamos el Alg