Quiz 6, April 1, 2002

This quiz concerns the Discrete Logarithm.

Example: Let $p = 7$ and $g = 3$. Then $Z_p = \{0, 1, 2, 3, 4, 5, 6\}$. The operations in $Z_p$ are: $4 \times 3 = 5$, $1 - 2 = -1 = 6$. Also,

$$g^0 = 1, g^1 = 3, g^2 = 2, g^3 = 6, g^4 = 4, g^5 = 5, g^6 = 1.$$ 

Observe that $6 = p - 1$. If this happens we say that $g$ is a generator of $Z_p$.

The Discrete Logarithm of 6 base 3 is 3: we write $log_3(6) = 3$.

Let $p = 11$ and $g = 2$.

List the elements of $Z_{11}$: $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

In $Z_{11}$:

1. $5 \times 4 = 9$
2. $2 - 1 = 1$
3. $g^2 = 2, g^3 = 8$
4. $g^4 = 5, g^5 = 10$
5. $g^6 = 9, g^7 = 7$
6. $log_2(4) = 2, log_2(7) = 7$

Is $g = 2$ a generator of $Z_{11}$? $\forall \in \mathbb{S}$