

Quiz 3 (Solutions); Friday, February 8, 2008

Determine whether or not the (multiplicative) group $U(7)$ is cyclic. Provide a detailed justification of your answer.

Solution. We have

$$U(7) = \{[n]_7 \mid \gcd(n, 7) = 1\} = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}.$$

To decide if $U(7)$ is cyclic we need to list all cyclic subgroups of $U(7)$ and check if any of them is equal to $U(7)$.

We have $2^2 = 4$ and $2^3 = 8 \equiv 1 \pmod{7}$, so that $[2^3]_7 = [1]_7$. Thus $[2]_7$ has order 3 in $U(7)$ and

$$\langle [2]_7 \rangle = \{[1]_7, [2]_7, [4]_7\} \neq U(7).$$

We next compute $\langle [3]_7 \rangle = \{[3^n]_7 : n \in \mathbb{Z}\}$. We have:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{7}, & [3^1]_7 &= [3]_7 \\ 3^2 &= 9 \equiv 2 \pmod{7}, & [3^2]_7 &= [2]_7 \\ 3^3 &\equiv 6 \pmod{7}, & [3^3]_7 &= [6]_7 \\ 3^4 &\equiv 18 \equiv 4 \pmod{7}, & [3^4]_7 &= [4]_7 \\ 3^5 &\equiv 12 \equiv 5 \pmod{7}, & [3^5]_7 &= [5]_7 \\ 3^6 &\equiv 15 \equiv 1 \pmod{7}, & [3^6]_7 &= [1]_7 \end{aligned}$$

Hence

$$U(7) = \langle [3]_7 \rangle,$$

so that $U(7)$ is cyclic.