Ancora sui sottogruppi ciclici

Ricordiamo anzittutto che, in un gruppo ciclico finito di ordine n, per ogni divisore positivo d di n esiste uno ed un solo sottogruppo (anch'esso ciclico) avente ordine d. Ciò implica, in particolare, che, in tale gruppo, elementi aventi lo stesso periodo generano lo stesso sottogruppo.
Inoltre, un elemento del gruppo ciclico finito appartiene ad un suo sottogruppo se (e solo se) il suo periodo divide l'ordine del sottogruppo.
Sia G un gruppo moltiplicativo generato dall'elemento periodico $g,$ di periodo n. Sia k un intero. Dalla formula del periodo segue allora che

1.) $\langle g^k \rangle = \langle g^{\mathrm{MCD}(n,k)} \rangle$

Pertanto, ogni sottogruppo ciclico di G è generato da una potenza di g avente come esponente un divisore di n (proprietà che, per altro, è nota per altra via, dato che, se d è l'ordine del sottogruppo, allora esso è generato da $g^{\frac{n}{d}}$, elemento di periodo d in base alla stessa formula del periodo).

Siano ora $h,\ k$ interi. Proviamo che

2.) $\langle g^h \rangle \cap \langle g^k \rangle = \langle g^{\mathrm{mcm}(h,k)} \rangle$.

L'inclusione $\supset$ è evidente. Proviamo $\subset$. Poniamo $h' = \mathrm{MCD}(n,h),\ k' = \mathrm{MCD}(n,k),$ così che $\langle g^{h'} \rangle = \langle g^h \rangle$, $\langle g^{k'} \rangle = \langle g^k \rangle$. Sia d un divisore (positivo) di n. Allora g^d appartiene al gruppo intersezione se (e solo se) il suo ordine, che è $\frac{n}{d}$, divide entrambi gli ordini di $g^{h'}$ e di $g^{k'}$, ossia entrambi i numeri interi $\frac{n}{h'}$ e $\frac{n}{k'}$. Ciò avviene se (e solo se) h' e k' dividono d, il che è verificato da $d = \mathrm{mcm}(h,k)$: infatti h' divide h e k' divide k. Ciò conclude la dimostrazione.