No:

Date:

C6

T1. 证明：(1) 由 $\delta_p(a)=3$ 可知 $a \bmod p \neq 1$，故 $p \nmid a-1$，$(a-1,p)=1$，由 $(a-1)\sum_{k=0}^{3} a^k = a^4-1 \equiv a-1 \bmod p$，故有 $\sum_{k=0}^{3} a^k \equiv 1 \bmod p$.

(2) 由 $\delta_p(a)=3$ 得 $a^2 \not\equiv 1 \bmod p$，$a \not\equiv \pm 1 \bmod p$，同由(1)中方法可证 $1+a+a^2 \equiv 0 \bmod p$，所以 $1+a \not\equiv 1 \bmod p$，$(1+a)^2 = 1+2a+a^2 \equiv a \not\equiv 1 \bmod p$，$(1+a)^3 = a^3+3a^2+3a+1 \equiv 1+3(a^2+a+1)-2 \equiv -1 \bmod p$，故 $\delta_p(1+a)=6$.

T3. 证明：(1) 由已知得 $(ab,n)=1$，

由 $(ab)^{[\delta_n(a),\delta_n(b)]} = (a^{\delta_n(a)})^{\frac{[\delta_n(a),\delta_n(b)]}{\delta_n(a)}} (b^{\delta_n(b)})^{\frac{[\delta_n(a),\delta_n(b)]}{\delta_n(b)}} \equiv 1 \bmod n$

得 $\delta_n(ab) \mid [\delta_n(a),\delta_n(b)]$；

又 $(ab)^{\delta_n(ab)\delta_n(b)} \equiv (a)^{\delta_n(ab)\delta_n(b)} \equiv 1 \bmod n$，故 $\delta_n(a) \mid \delta_n(ab)\delta_n(b)$

从而有 $\frac{\delta_n(a)}{(\delta_n(a),\delta_n(b))} \mid \delta_n(ab)$，同理有 $\frac{\delta_n(b)}{(\delta_n(a),\delta_n(b))} \mid \delta_n(ab)$.

①充分性 ($\Leftarrow$)：$(\delta_n(a),\delta_n(b))=1$，则 $\delta_n(a) \mid \delta_n(ab)$，$\delta_n(b) \mid \delta_n(ab)$，得 $\delta_n(a)\delta_n(b) \mid \delta_n(ab)$，又 $(ab)^{\delta_n(a)\delta_n(b)} \equiv 1 \bmod n$，$\delta_n(ab) \mid \delta_n(a)\delta_n(b)$

所以 $\delta_n(ab) = \delta_n(a)\delta_n(b)$

②必要性 ($\Rightarrow$)：若 $\delta_n(ab) = \delta_n(a)\delta_n(b)$，则 $\delta_n(a)\delta_n(b) \mid [\delta_n(a),\delta_n(b)]$

即 $(\delta_n(a),\delta_n(b))[\delta_n(a),\delta_n(b)] \mid [\delta_n(a),\delta_n(b)]$，可知必有 $(\delta_n(a),\delta_n(b))=1$.

证毕.

Date:

T4.(1) 证明：对 $\forall k, 1 \le k \le \frac{p-1}{2}$，$(g^{2k})^{\frac{p-1}{2}} = (g^{p-1})^k \equiv 1 \bmod p$

所以 $g^2, g^4, \cdots g^{p-1}$ 为模 p 的二次剩余，故剩余 $\frac{p-1}{2}$ 个元素 $g, g^3 \cdots g^{p-2}$ 为模 p 的二次非剩余.

T6.(1) 证明：$2 \mid p-1$，故 $(-g)^{p-1} \equiv g^{p-1} \equiv 1 \bmod p$，下证 $\delta_p(g) = p-1$. 使用反证法，假设 $k = \delta_p(-g) \le p-2$，则必有 $2 \nmid k$. 否则

$$g^k = (-g)^k \equiv 1 \bmod p, \quad \delta_p(g) = k < p-1 \text{ 矛盾.}$$

又 $k \mid p-1$，$2 \nmid k$，得 $k \mid \frac{p-1}{2}$，由 $p \equiv 1 \bmod 4$，得 $2 \mid \frac{p-1}{2}$，从而有 $(-g)^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \equiv 1 \bmod p$，与 g 为原根矛盾！故 $k = p-1$，即 $-g$ 为 p 的原根.