No.

Date.　　/　　/

习题1：

①必要性，已知m为素数

由原根的定义，素数的乘法群是阿贝尔群，其生成元的次数即其原根的次数为$\phi(m)=m-1$.

②充分性，存在α的次数为$m-1$

若m不是素数，则$\phi(m)<m-1$，而拉格朗日定理表明任何元素的阶必须整除$\phi(m)$，因此不可能存在阶为$m-1$的元素。

习题2：

① $p\equiv 1 \pmod 4$　$\therefore -1$是模p的二次剩余，即$\exists k\in\mathbb{Z}$, $-1\equiv g^{2k} \pmod p$

$\therefore -g\equiv g\cdot g^{2k}=g^{2k+1} \pmod p$

若$(-g)^d\equiv 1 \pmod p$　$\because g$为原根且$g^m\equiv 1 \pmod p \Leftrightarrow m\equiv 0 \pmod{p-1}$

$\therefore (2k+1)d\equiv 0 \pmod{p-1}$　$\therefore d=\frac{p-1}{(2k+1,p-1)}=p-1$

$\therefore (-g)^{p-1}=(-g)^{\phi(p)}\equiv 1 \pmod p$　$\therefore -g$为原根

② $p\equiv 3 \pmod 4$　$\therefore -1$不是模p的二次剩余，且$(-1)^{\frac{p-1}{2}}\equiv -1 \pmod p$

$\because g$是原根　$\therefore g^{\frac{p-1}{2}}\equiv -1 \pmod p$

$\therefore (-g)^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}\cdot g^{\frac{p-1}{2}}\equiv (-1)\cdot(-1)=1 \pmod p$

假设 $\mathrm{ord}_p(-g)=d$ 且 $d<\frac{p-1}{2}$，则 $(-g)^d\equiv 1 \pmod p$

$\therefore (-1)^d g^d\equiv 1 \pmod p$

$\because g$是原根，$g^d=(-1)^d \pmod p$，但 $d<\frac{p-1}{2}$，这与g的阶为$p-1$矛盾

$\therefore d$最小为$\frac{p-1}{2}$

$\therefore -g$的阶为$\frac{p-1}{2}$

No.
Date. / /

习题15：

$a^n \equiv 1 \pmod{a^n-1}$

$\therefore ord_{a^n-1}(a)=n$ $\quad \because gcd(a,a^n-1)=gcd(a,-1)=1$

$\therefore$ 由欧拉定理 $a^{\phi(a^n-1)} \equiv 1 \pmod{a^n-1}$

$\therefore$ 由拉格朗日定理 $n \mid \phi(a^n-1)$

61：① 原根个数为 $\varphi(17-1)=\varphi(16)=16\times\frac{1}{2}=8$

② 若 x 的次数为4，则 $x^4 \equiv 1 \pmod{17}$

通过验证，$x=4,13,16$

62：① $x^6 \equiv 5 \pmod{17}$

取原根 $g=3$，设 $x \equiv 3^k \pmod{17}$，则 $3^{6k} \equiv 5 \pmod{17}$

查表得 $ind_3(5)=5$ $\therefore 6k \equiv 5 \pmod{16}$

$\therefore k = 5 \cdot 6^{-1} \equiv 15 \pmod{16}$

$\therefore x \equiv 3^{15} \equiv 6 \pmod{17}$

② $3^x \equiv 7 \pmod{17}$

查表得 $ind_3(7)=11$

$\therefore x \equiv 11 \pmod{16}$