No.

Date. / /

习题5.22

(a) 1. $\forall a, b \in G(n)$

则 $\left(\frac{ab}{n}\right) \equiv a^{\frac{n-1}{2}} \times b^{\frac{n-1}{2}} = (ab)^{\frac{n-1}{2}} \pmod n$

$\therefore ab \in G(n)$

2. $\forall a \in G(n)$

$\exists a^{-1} \in Z_n^*$ 满足 $\left(\frac{a^{-1}}{n}\right) \equiv \left(\frac{a}{n}\right)^{-1} \equiv a^{-\frac{n-1}{2}} \pmod n$

且 $(a^{-1})^{\frac{n-1}{2}} \equiv a^{-\frac{n-1}{2}} \pmod n$ $\therefore a^{-1} \in G(n)$

$\therefore$ 综上所述，$G(n)$ 是 Z_n^* 的一个子群

(d) 1. 若 $n = p^k$

由(a)知 $G(n)$ 为真子群，故 $|G(n)| \le \frac{\phi(n)}{2} \le \frac{n-1}{2}$

2. 若 $n = p_1^{e_1} \cdots p_s^{e_s}$

则由(c)知，$\exists a \in Z_n^*$ 使得 $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod n$，故 $G(n) \neq Z_n^*$

$\therefore$ 由(a)知 $|G(n)| \le \frac{n-1}{2}$

(e) 由(d)，若 n 为奇合数，则 $G(n) = \{a \in Z_n^* \mid \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod n\}$ 的大小满足 $|G(n)| \le \frac{n-1}{2}$

则对合数 n，随机选取的 $a \in G(n)$ 的概率为 $\frac{|G(n)|}{n-1} \le \frac{\frac{n-1}{2}}{n-1} = \frac{1}{2}$

$\therefore$ 第一次错误接受 n 为素数的概率 $\le \frac{1}{2}$

若重复 k 次测试，则错误概率降至 $\le \frac{1}{2^k}$