Date. / / / MAC	
习题 5.22	
(a) 1. Ya, be G(n)	
N (함) = a 보 b = (ab) = (mod	n)
2 ab e G(n)	
2. ∀a∈G(n)	
∃a-1€Z* 満足(雪)=(品)-1= a-当	(mod n)
$\mathbb{E}\left(a^{-1}\right)^{\frac{n-1}{2}} \equiv a^{-\frac{n-1}{2}} \pmod{n} \text{i. } a^{-1} \in$	
与综上所述,G(n)是Zn*的一个子群	
X x X x 2 = 12	S. S. Markers . S. A. A.
(d) 1.若n=pk	A THE FRIENCE VEX SHE
由(a)知G(n)为真子群,故(G(n))<处	<u> </u>
2. 若n= pe pes	X III =
则由(c)知, 且QE Zn*使得(A) +	$\alpha^{\frac{n-1}{2}} \pmod{n}$, 故 $G(n) \neq Z_n^*$
- 由 (a) 412 G(n)] ≤ n-1/2	MATA TIME
(e) 由(d), 若n为奇台数, 则 G(n)= {aeZ*	* (条)=a ^竖 (modn)} 的大小满足 G(n) <笠
IN 对合数n,随机线取动 a EG(n)的标	既产为 G(n) < 型 = - 1
5. 第一次特误接受n为素数的概率<=>	(2) VXCP 14 EC
若重复k次测试,则错误概率降至。	EZE PER THINK ENERGY
	CETTE Z. PRINCESSE
	Being Frankland Mets
	1 to 1

REMEMBER MEMORY