13.2 a)

$(987^{911}) \bmod 911$

$\varphi(911) = 910$

$a^k = a^{k \bmod |G|}$

$(987 \bmod 911)^{911 \bmod 910} = 76^1 = 76$

$\langle \mathbb{Z}_{911}^*, \cdot_{911}, 1 \rangle$

$(987^{909}) \bmod 911 =$

$(987 \bmod 911)^{909 \bmod 910}$

76^{-1}

a	b	k	s	t
76	911	11	12	-1
75	76	1	-1	1
1	75	—	1	0

$12 \cdot 76 = 1$

$76^{-1} \equiv_{911} 12$

b) $\pi = (1,2,3)(4,5)$ $\quad \pi^{787}, \pi^{785}$

$ord(\pi) = k \, GV(2,3) = 6$

	π	π^2
1	2	3
2	3	1
3	1	2
4	5	4
5	4	5

$$a^k = a^{k \bmod ord(a)}$$

$$\pi^{787} = \pi^{787 \bmod 6} = \pi^1$$

$$\pi^{785} = \pi^{-1} = (1,3,2)(4,5)$$

13.3a) Untergruppe von $\mathbb{Z}_{20}^*$ bilden mit $\langle 3 \rangle$

$\Rightarrow$ 3 ist Erzeuger $ord(3) = |\langle 3 \rangle|$

$|\langle 3 \rangle|$ ist Teiler von $\mathbb{Z}_{20}^*$

$$\varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$$

$3^2 \bmod 20 = 9$

$3^4 \bmod 20 = 1 \quad \rightarrow ord(3) = 4$

b) $\varphi(34) = \varphi(2) \cdot \varphi(17) = 16$

$3^2 \equiv_{34} 9$, $3^4 \equiv_{34} 13$, $3^8 \equiv_{34} 13^2 \equiv_{34} 33$

$3^{16} \equiv_{34} 1$

c) $(1,2,4)(3,5)$ → siehe 13.2b)

$ord(\pi) = 6$

d) kGV aller Elementordnungen → $kGV(1,2,4) = 4$

$2 \in \mathbb{Z}_{34}^*$ ← 2.17

e) $2 \cdot p^r$ p ∉ P r ∈ Z

→ $\mathbb{Z}_{34}^*$ ist zyklisch

→ Gruppenexponent $|\mathbb{Z}_{34}^*| = 16$

f) Die Ordnung einer Permutation ist

das kGV der Zyklenlängen

→ $kGV(1,2,3,4,5) = 60$

13.4 a) a ist Erzeuger von G_1

gdw $a^{|G|/p} \neq 1$ für jeden Primfaktor in $|G|$

$|\mathbb{Z}_{89}^*| = \varphi(89) = 88 = 2^3 \cdot 11$

$3^{\frac{88}{2}} \equiv_{89} 3^{44} \equiv_{11} 81^{11} \equiv_{89} (-8)^{11} \equiv_{89} (-2)^{33} \equiv_{89} -(2^{10})^3 \cdot 2^3 = (1024)^3 \cdot 8 \equiv_{89} -(45)^2 \cdot 8 =$

$-3^6 \cdot 5^3 \cdot 2^3 \equiv_{89} -81 \cdot 9 \cdot 125 \cdot 8 \equiv_{89} 8 \cdot 9 \cdot 36 \cdot 8 \equiv_{89} -1$

$3^{\frac{88}{11}} = 3^8 = (3^4)^2 = 81^2 \equiv_{89} (-8)^2 = 64$

b) $s^{\frac{88}{2}} = s^{44} = (s^4)^{11} = (125 \cdot s)^{11} \equiv_{89} (36 \cdot 5)^{11} \equiv_{89} 2^{11} = 2048 \equiv_{89} 1$

c) $ord(3) = 88 \qquad 3^{88/22} = 3^4 = 81 \leftarrow ord(81) = 22$

d) 12 ist kein Teiler von 88 $\rightarrow$ es gibt kein Element

$\langle \mathbb{Z}_{20}^*, \cdot_{20}, 1 \rangle$ $\qquad \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{1, 3, 9, 7\}$