dem Exponenten γ gehören möge, v das kleinste Vielfache von ε, γ. Es gibt ein Potenzprodukt $b^\rho c^\sigma$, welches nach n zu dem Exponenten v gehört. Denn der größte gemeinschaftliche Teiler δ der Zahlen ε, γ besitzt einen größten zu $\frac{\gamma}{\delta}$ teilerfremden Teiler ρ und es sei $\delta = \rho\sigma$, wo σ in einer Potenz von $\frac{\gamma}{\delta}$ aufgehen muß. b^ρ, c^σ gehören nach n beziehungsweise zu den Exponenten $\frac{\gamma}{\rho}$, $\frac{\varepsilon}{\sigma}$ und daher, da letztere teilerfremd sind, $b^\rho \sigma^\sigma$ zu dem Exponenten $\frac{\gamma}{\rho} \cdot \frac{\varepsilon}{\sigma} = \frac{\varepsilon\gamma}{\delta} = v$.

Da der kleinste nicht negative Rest von $b^\rho c^\sigma$ in bezug auf n in der Reihe (1) vorkommt, so kann v nicht $> \varepsilon$ sein. Daher ist $v = \varepsilon$, γ ein Teiler von ε.

Wird das Zeichen ind auf eine primitive Kongruenzwurzel des Moduls n bezogen, so ist $\operatorname{ind} c = q \frac{\varphi(n)}{\varepsilon}$, wo q zu ε teilerfremd ist, und daher

$$\frac{\varphi(n)}{\varepsilon} \equiv m \operatorname{ind} c \pmod{\varphi n},$$

wo m eine ganze Zahl bedeutet. Hieraus folgt, da $\operatorname{ind} b$ ein Vielfaches von $\frac{\varphi(n)}{\gamma} = \frac{\varepsilon}{\gamma} \frac{\varphi n}{\varepsilon}$ ist

$$\operatorname{ind} b \equiv k \operatorname{ind} c \quad (\varphi(n)),$$

wo k eine ganze Zahl bezeichnet. Somit ist

$$b \equiv c^k (n)$$

und die Zahlen (1) fallen mit den kleinsten nicht negativen Resten der Potenzen

$$1, c, c^2, \ldots c^{\varepsilon-1} \tag{2}$$

in bezug auf den Modul n zusammen. Der kleinste nicht negative Rest der Potenzen c^h, $c^{\varepsilon-h}$ in bezug auf den Modul n werde mit c_h, c_{-h} bezeichnet.