§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0, g^1, g^2 \ldots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschluss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ, die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl* n *für die Basis* g, und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c, so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. }(1) \equiv 0, \quad \text{Ind. }(-1) \equiv \tfrac{1}{2}c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind.} n} \pmod{p^\pi}$$

folgt nämlich