Mit Hülfe dieses allgemeinen Resultates sind wir im Stande zu beurtheilen, ob die Congruenz

$$x^2 \equiv D \pmod{k},$$

in welcher D und k relative Primzahlen sind, möglich, und wie gross die Anzahl σ ihrer incongruenten Wurzeln ist. Bedeutet p jede beliebige in dem Modul k (also nicht in D) aufgehende ungerade Primzahl, so ist erforderlich, dass

$$\left(\frac{D}{p}\right) = +1$$

sei; ist diese Bedingung erfüllt, so hat die Congruenz $x^2 \equiv D$ in Bezug auf jeden Modulus von der Form p^π genau zwei incongruente Wurzeln. Ist daher der Modul k ungerade, und μ die Anzahl der von einander verschiedenen in k aufgehenden Primzahlen p, so ist

$$\sigma = 2^\mu.$$

Dasselbe ist der Fall, wenn der Modulus k das Doppelte einer ungeraden Zahl ist; denn die Congruenz $x^2 \equiv D \pmod{2}$ hat stets eine und nur eine Wurzel.

Ist aber k das Vierfache einer ungeraden Zahl, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod{4}$ sei; da alsdann die Congruenz $x^2 \equiv D \pmod{4}$ zwei Wurzeln besitzt, so ist

$$\sigma = 2^{\mu+1}.$$

Ist endlich $k \equiv 0 \pmod{8}$, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod{8}$ sei; da dann die Congruenz $x^2 \equiv D \pmod{2^\pi}$, wo $\pi \geqq 3$, stets vier Wurzeln hat, so ist in diesem Fall

$$\sigma = 2^{\mu+2}.$$

§. 38.

Bevor wir diesen Gegenstand verlassen, wollen wir noch eine Anwendung von dem soeben gewonnenen Resultate auf eine Verallgemeinerung des Wilson'schen Satzes (§. 27) machen. Setzen wir $D = 1$, so ergiebt sich, dass die Congruenz

$$x^2 \equiv 1 \pmod{k} \tag{1}$$