durch Potenzirung mit allen zu $\delta$ theilerfremden Zahlen entstehen, und die $\delta^{ten}$ Potenzen derselben nach dem Modul $p$ congruent 1 sein. Sie gehören aber geradezu zum Exponenten $\delta$ selbst; denn würde eine Wurzel $\alpha$ der Congruenz 3), also auch jede, zu einem Exponenten $\delta' < \delta$ gehören, so könnte dieser nur ein Theiler von $\delta$ sein, und da dann im Allgemeinen $\varphi(\delta') < \varphi(\delta)$ ist, so besässe die Congruenz 3) nicht lauter verschiedene Wurzeln; ist jedoch $\varphi(\delta') = \varphi(\delta)$, d. h. $\delta = 2\delta'$, wobei $\delta'$ ungerade sein muss, so wäre schon $\alpha^{\frac{\delta}{2}} \equiv 1 \bmod p$, was nach dem eben erwähnten Kummer'schen Satze nicht sein kann, weil die $\frac{\delta^{te}}{2}$ Potenz einer primitiven $\delta^{ten}$ Einheitswurzel gleich $-1$ ist.

Ist also $p$ eine Primzahl, $\delta$ ein Theiler von $p-1$, so besitzt die Gleichung für die primitiven $\delta^{ten}$ Einheitswurzeln, als Congruenz nach dem Modul $p$ aufgefasst, alle modulo $p$ zum Exponenten $\delta$ gehörigen Zahlen zu Lösungen. Speciell: Die Gleichung für die primitiven $(p-1)^{ten}$ Einheitswurzeln, als Congruenz nach dem Modul $p$ aufgefasst, besitzt die sämmtlichen primitiven Wurzeln von $p$ als Lösungen.

Nun ergeben sich die eingangs angeführten Sätze von Gauss unmittelbar durch Anwendung des vorhin erwähnten Kummer'schen Satzes; der erste, bezüglich des Productes aller primitiven Wurzeln, aus dem Umstande, dass das Product sämmtlicher Wurzeln der Gleichung $\Phi_p(x) = 0$ gleich 1 ist, wobei der Fall $p = 3$ desshalb eine Ausnahme bildet, weil hier allein der Grad der Gleichung für die primitiven $(p-1)^{ten}$ Einheitswurzeln ein ungerader, das Product der Wurzeln also gleich dem negativen letzten Gliede wird; der zweite, bezüglich der Summe, als specieller Fall der allgemeinen Formel für die $k^{te}$ Potenzsumme der Wurzeln irgend einer Kreistheilungsgleichung $\Phi_m(x) = 0$, die bekanntlich folgende ist:

$$S_k = (-1)^r . m' . \varphi(Q) \quad \text{oder} \quad S_k = 0, \qquad 4)$$

je nachdem $k$ durch $m'$ theilbar ist oder nicht. (Hiebei ist für den ersten Fall $m = m'.P$, $P$ das Product aller verschiedenen in $m$ aufgehenden Primzahlen, $k = m'.K$, $Q$ der grösste Theiler der Zahlen $K$ und $P = Q.R$, endlich $r$ die Anzahl der in $R$ enthal-