III. Die Darstellung einer ganzen Zahl als Summe von höchstens vier Quadraten.

Von **Alexander Witting.**

Vorbemerkung. Die nachfolgende Darstellung ist ein Teil des am 21. Oktober 1920 in der Mathematischen Sektion der Isis gehaltenen Vortrags „Uber die Darstellung einer ganzen Zahl als Summe gleichhoher Potenzen“, in dem eine Übersicht über das bis jetzt Bekannte gegeben wurde. Auf besonderen, von verschiedenen Seiten geäußerten Wunsch erfolgt die Veröffentlichung des folgenden Beweises, der absichtlich in voller Ausführlichkeit dargestellt ist, um auch denen zugänglich zu sein, die nicht mit der elementaren Zahlentheorie vertraut sind.

I. Unter den Primzahlen spielt die 2 eine besondere Rolle, wir wollen sie daher zunächst nicht mit betrachten, sondern unter p eine ungerade Primzahl verstehen. Wir fassen nun irgend zwei verschiedene positive, ganze Zahlen x und y ins Auge und fragen, wann die Differenz ihrer Quadrate durch p teilbar ist; ist also m eine positive ganze Zahl, so wird dann die Gleichung bestehen

$$1.)\quad x^2 - y^2 = mp.$$

Da aber $x^2 - y^2 = (x+y)\,(x-y)$ ist, so muß p ein Faktor entweder von $x+y$ oder von $x-y$ sein.

Nehmen wir jetzt an, daß x und y beide kleiner als p sind, so folgt notwendig, daß $x+y=p$ ist, wir können also die beiden Zahlen x und y in der Form

$$2.)\quad x = \frac{p-1}{2} - k,\quad y = \frac{p-1}{2} + k + 1$$

darstellen, d. h. aber: zwei Zahlen x und y, kleiner als p, die der Bedingung 1.) genügen, liegen symmetrisch zur Mitte in der Reihe der Zahlen von 1 bis $p-1$. Die Bedingung 1.) sagt aber zugleich aus, daß die beiden Quadrate x^2 und y^2 bei der Division durch p denselben Rest lassen, denn die Differenz $x^2 - y^2$ soll ja durch p teilbar sein. Es folgt demnach der Satz, daß die Quadrate der Zahlen $1, 2, 3 \ldots p-1$ nur $\frac{p-1}{2}$ verschiedene Reste bei der Division durch p ergeben, die symmetrisch angeordnet sind.

Man spricht daher von den $\frac{p-1}{2}$ quadratischen Resten modulo p.

Sei z. B. $p = 13$, so ergibt sich folgende Tabelle:

Zahlen	1	2	3	4	5	6	7	8	9	10	11	12
Quadrate	1	4	9	16	25	36	49	64	81	100	121	144
Reste	1	4	9	3	12	10	10	12	3	9	4	1.