Über die Darstellung der Zahlen als Summe von vier Quadraten.

Von **R. Daublebsky von Sterneck** in Wien.

Aus der Identität:

$$(a^2+b^2+c^2+d^2)\ (\alpha^2+\beta^2+\gamma^2+\delta^2) =$$
$$=(a\alpha+b\beta+c\gamma+d\delta)^2+(a\beta-b\alpha-c\delta+d\gamma)^2+$$
$$+(a\gamma+b\delta-c\alpha-d\beta)^2+(a\delta-b\gamma+c\beta-d\alpha)^2$$

erschließt man erstens, daß man, um zu beweisen, daß jede ganze Zahl die Summe von vier (oder weniger) Quadratzahlen ist, dies nur für Primzahlen zu beweisen braucht. Da ferner die Primzahl 2 offenbar eine solche Darstellung zuläßt, so kann man sich darauf beschränken, den Satz für ungerade Primzahlen p zu beweisen.

Lagrange hat ferner gezeigt, daß aus obiger Identität auch gefolgert werden kann, daß die ungerade Primzahl p, sobald sie in der Summe von vier Quadraten aufgeht, selbst in dieser Form darstellbar ist.[1])

Der Beweis des Satzes, daß jede ganze Zahl als Summe von vier Quadraten dargestellt werden kann, reduziert sich also darauf, zu zeigen, daß jede ungerade Primzahl p in der Summe von vier oder weniger Quadraten aufgeht. Hiezu sind verschiedene Methoden verwendet worden; so hat Euler im 5. Bande der Novi Commentarii der Petersburger Akademie bewiesen, daß jede Primzahl in der Formel t^2+u^2+1 aufgeht. Etwas allgemeiner hat Lagrange in den Abhandlungen der Berliner Akademie bewiesen, daß jede Primzahl in der Formel t^2-Bu^2-C aufgeht, wenn B und C beliebige durch die Primzahl unteilbare Zahlen sind.[2])

Während diese Beweise immerhin einige zahlentheoretische Kenntnisse voraussetzen, wie etwa u. a. den Satz, daß eine Kongruenz nach einem Primzahlmodul niemals mehr Wurzeln haben kann, als

---

[1]) Vgl. Legendre, Zahlentheorie, deutsch von Maser, 1. Band 1886. S. 215.
[2]) Legendre, Zahlentheorie. 1. Band. S.212.

der Grad anzeigt, kann man auch mit noch einfacheren Mitteln auskommen. So finden sich in dem neu erschienenen Buche von Wertheim [1]) zwei Beweise, welche sich auf einfache Bemerkungen über die Verteilung der quadratischen Reste in der Reihe $0, 1, 2, \ldots, p-1$ gründen und zum Teile von A. Matrot gelegentlich des Kongresses der „Association française pour l'avancement des sciences" zu Limoges 1890 veröffentlicht wurden.

Im folgenden möchte ich mir erlauben, eine noch einfachere Schlußweise mitzuteilen, die ich mir zu Vorlesungszwecken zurechtgelegt habe und die bloß mit dem Begriffe des quadratischen Restes und Nichtrestes sowie dem Satze auskommt, daß das Produkt zweier Reste oder zweier Nichtreste ein Rest, das Produkt eines Restes und eines Nichtrestes aber ein Nichtrest ist. Man kann nämlich die Tatsache, daß jede ungerade Primzahl p entweder in der Summe zweier oder dreier Quadrate aufgeht, in folgender Weise erschließen:

Es sollen $R, R', R'', \ldots$ quadratische Reste, $N, N', N'', \ldots$ quadratische Nichtreste (mod p) bezeichnen.

Ist -1 quadratischer Rest der Primzahl p, so ist $-R'$ ein Rest, also

$$R \equiv -R' \pmod{p}$$

oder

$$R + R' \equiv 0 \pmod{p}$$

also gibt es in diesem Falle zwei Quadrate, deren Summe durch p teilbar ist.

Ist -1 quadratischer Nichtrest der Primzahl p, so muß es immer zwei quadratische Reste geben, deren Summe einem Nichtreste kongruent ist; denn wäre für je zwei beliebige Reste immer

$$R + R' \equiv R'' \pmod{p}$$ [2])

so würde durch beiderseitige Addition eines Restes folgen:

$$R + R' + R''' \equiv R'' + R''' \equiv R^{IV} \pmod{p};$$

ebenso wäre die Summe von vier beliebigen Resten immer wieder ein Rest, und durch Fortsetzung desselben Verfahrens fände man schließlich, daß die Summe von i ganz beliebigen quadratischen Resten immer wieder ein Rest wäre:

$$R + R' + R'' + \ldots + R^{(i-1)} \equiv R^{(i)} \pmod{p}.$$

Macht man nun aber die spezielle Annahme, daß

$$R = R' = R'' = \ldots = R^{(i-1)}$$

---

[1]) Wertheim, Anfangsgründe der Zahlenlehre. Braunschweig 1902. S. 396.

[2]) Der Fall $R + R' \equiv 0 \pmod{p}$ schließt sich hier von selbst aus, da -1 als quadrat. Nichtrest (mod. p) vorausgesetzt ist.

sei, und nimmt für i einen Nichtrest, so käme man auf den Widerspruch

$$i \,.\, R \equiv R^{(i)} \pmod{p},$$

so daß also das Produkt aus einem Nichtreste und einem Reste ein Rest wäre. Es muß also jedenfalls zwei quadratische Reste geben, deren Summe einem Nichtreste kongruent ist

$$R + R' \equiv N \pmod{p}.$$

Nun ist aber -1 quadratischer Nichtrest; es ist daher:

$$-N \equiv R'' \pmod{p},$$

so daß die Beziehung besteht:

$$R + R' + R'' \equiv 0 \pmod{p}.$$

Es gibt also in der Tat drei quadratische Reste, mithin auch drei Quadrate, deren Summe durch p teilbar ist, womit der Satz nun auch in diesem Falle bewiesen ist.[1])

Gelegentlich einer Durchsicht des handschriftlichen Nachlasses des Prager Philosophen und Mathematikers Bernhard Bolzano (gestorben 1848) fand ich durch Zufall eine Notiz vor, die sich ebenfalls auf die Darstellbarkeit der Zahlen als Summe von vier Quadraten bezieht. Daselbst wird in der allereinfachsten Weise der Hilfssatz Lagranges bewiesen, daß es immer zwei Zahlen t und u gibt, welche der Bedingung

$$t^2 - Bu^2 - C \equiv 0 \pmod{p}$$

genügen, wenn B und C irgendwelche durch p unteilbare Zahlen bedeuten. Für die Werte $t = 0, 1, 2, \ldots \frac{p-1}{2}$ durchläuft nämlich t^2 $\frac{p+1}{2}$ inkongruente Werte (mod. p) und ebenso durchläuft für $u = 0, 1, 2, \ldots \frac{p-1}{2}$ der Ausdruck $Bu^2 + C$ $\frac{p+1}{2}$ inkongruente Werte (mod. p). Es muß nun mindestens einer der ersteren Werte mit einem der letzteren (mod. p) übereinstimmen, da es sonst $p+1$ inkongruente Werte (mod. p) geben müßte.[2]) Für die betreffenden Werte t und u wird daher

$$t^2 \equiv Bu^2 + C \pmod{p}$$

---

[1]) Das Resultat ist nur ein spezieller Fall des Satzes von Lebesgue (Recherches sur les nombres, Liouv. J. 2) über die Anzahl der Wurzeln der Kongruenz $a_1 y_1^2 + a_2 y_2^2 \equiv \alpha \pmod{p}$, worauf mich Herr Professor P. Bachmann aufmerksam zu machen die Güte hatte.

[2]) Eine dieser Bolzanoschen verwandte Schlußweise mit demselben Grundgedanken findet sich in Bachmanns „Arithmetik der quadratischen Formen" 1. Abt. Leipzig 1898. S. 488.

oder also

$$t^2 - Bu^2 - C \equiv 0 \pmod{p}.$$

Indem man $B = C = -1$ setzt, geht daraus hervor, daß jede Primzahl p in der Summe dreier Quadrate aufgeht.

Auch dieser Bolzanosche Beweis scheint so nahe zu liegen, daß es fast Wunder nimmt, dieselbe Sache bei Lagrange in so umständlicher Weise behandelt zu finden.