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 „Über 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.

Nehmen wir noch die Zahl 0 hinzu, so ergeben die Quadrate von x, wenn es die Folge der Zahlen 0, 1, 2, 3 . . ., $p-1$ durchläuft, genau $\frac{p-1}{2}+1=\frac{p+1}{2}$ (mod. p) inkongruente Zahlen — man nennt nämlich zwei Zahlen, die bei der Division durch p denselben Rest lassen, kongruent modulo[1] p; zwei Zahlen, die nicht denselben Rest lassen, heißen (mod. p) inkongruent.

II. Sei nun B irgendeine positive oder negative ganze Zahl mit Ausnahme der Vielfachen von p, dann überzeugt man sich leicht, daß der Ausdruck By^2, wenn y die Folge 0, 1, 2, . . . $p-1$ durchläuft, auch wieder genau $\frac{p+1}{2}$ (mod. p) inkongruente Zahlen ergibt. Addiert man endlich eine beliebige positive oder negative ganze Zahl C, so wird der Ausdruck By^2+C, wenn y die oben erwähnte Folge von Zahlen durchläuft, ebenso wieder $\frac{p+1}{2}$ (mod. p) inkongruente Zahlen ergeben, d. h. also, man erhält auch hier wieder $\frac{p+1}{2}$ verschiedene quadratische Reste (mod. p). Sind nun diese Reste verschieden von den Resten, die x^2 beim Durchlaufen jener Zahlenfolge aufweist, oder anders ausgedrückt: Sind die Zahlen By^2+C allen Zahlen x^2 inkongruent? Wenn das stattfände, so hätte man $\frac{p+1}{2}+\frac{p+1}{2}=p+1$ (mod. p) inkongruente Zahlen; das ist aber unmöglich, denn es gibt nur p solcher Zahlen. Daher muß mindestens eine der Zahlen By^2+C einer Zahl x^2 (mod. p) kongruent sein[2]. Es muß daher mindestens zwei Zahlen x und y geben, sodaß $x^2-(By^2+C)$ ein Vielfaches von p wird.

III. Wir nehmen nun 1.) $B=C=-1$ und erhalten mindestens zwei Zahlen x und y, für welche x^2+y^2+1 ein Vielfaches von p ist.

Wir nehmen ferner 2.) $B=-1$, $C=+1$ und erhalten mindestens zwei Zahlen z und t, für welche z^2+t^2-1 ein Vielfaches von p ist.

Daraus aber ergibt sich, daß die Summe jener beiden Ausdrücke: $x^2+y^2+z^2+t^2$ ebenfalls ein Vielfaches von p ist[3], d. h. es gibt immer vier Zahlen x, y, z, t von der Art, daß

$$3.)\quad x^2+y^2+z^2+t^2=pm$$

ist. Dabei brauchen allerdings diese Zahlen nicht alle voneinander verschieden zu sein. Wir können weiter sagen, daß die Zahlen x, y, z, t nicht alle durch m teilbar sind, denn dann wäre ja die Summe durch m^2 teilbar, was unmöglich ist, da p eine Primzahl ist.

IV. Wir nehmen jetzt vier beliebige ganze Zahlen ξ, η, ζ, ϑ; dann besteht die Gleichung:

$$4.)\quad (x-p\xi)^2+(y-p\eta)^2+(z-p\zeta)^2+(t-p\vartheta)^2=pm'.$$

---

[1] Modulo p, also „nach dem Modul p", wird stets (mod. p) abgekürzt.

[2] Beispiel für $p=13$: $5y^2+3$ ergibt die Reste 3, 8, 10, 9, 5, 11, 1 für $y=0, 1, \ldots 6$. Man vergleiche!

[3] So ist z. B. $3^2+4^2+1=2\cdot 13$, $2^2+6^2-1=3\cdot 13$, also $2^2+3^2+4^2+6^2=5\cdot 13$.

Wählt man die Zahlen ξ, η, ζ, ϑ so, daß $x - p\xi$ usw. ohne alle zu verschwinden, absolut kleiner als $\frac{p}{2}$ werden, dann ist $pm' < 4 \cdot \frac{p^2}{4}$, also $m' < p$. Wir können also gleich in 3.) das $m < p$ voraussetzen.

Nun nehmen wir irgend vier neue ganze Zahlen x_1, y_1, z_1, t_1 und erhalten aus 3.) die Gleichung

5.) $(x - mx_1)^2 + (y - my_1)^2 + (z - mz_1)^2 + (t - mt_1)^2 = mm_1$.

Dann kann man x_1, y_1, z_1, t_1 so wählen, daß $x - mx_1$ usw. ohne alle zu verschwinden absolut kleiner als $\frac{m}{2}$ werden; mithin wird $mm_1 < 4 \cdot \frac{m^2}{4}$, also[1] $m_1 < m$.

V. Man rechnet leicht aus, daß die folgende Identität besteht:

6.) $(x^2 + y^2 + z^2 + t^2)(\xi^2 + \eta^2 + \zeta^2 + \vartheta^2)$
$= (x\xi + y\eta + z\zeta + t\vartheta)^2 + (x\eta - y\xi + z\vartheta - t\zeta)^2$
$+ (x\zeta - z\xi - y\vartheta + t\eta)^2 + (x\vartheta - t\xi + y\zeta - z\eta)^2$

d. h. zwei Summen von je vier Quadraten ergeben mit einander multipliziert abermals eine Summe von vier Quadraten.

Multipliziert man daher die Gleichungen 3.) und 5.) mit einander, so erhält man:

$$(x^2+y^2+z^2+t^2)\left[(x-mx_1)^2+(y-my_1)^2+(z-mz_1)^2+(t-mt_1)^2\right] = pm^2m_1$$
$$= \left[x(x-mx_1)+y(y-my_1)+z(z-mz_1)+t(t-mt_1)\right]^2$$
$$+ \left[x(y-my_1)-y(x-mx_1)+z(t-mt_1)-t(z-mz_1)\right]^2$$
$$+ \left[x(z-mz_1)-z(x-mx_1)-y(t-mt_1)+t(y-my_1)\right]^2$$
$$+ \left[x(t-mt_1)-t(x-mx_1)+y(z-mz_1)-z(y-my_1)\right]^2$$
$$= \left[pm - m(xx_1+yy_1+zz_1+tt_1)\right]^2 + \left[-m(xy_1-yx_1+zt_1-tz_1)\right]^2$$
$$+ \left[-m(xz_1-zx_1-yt_1+ty_1)\right]^2 + \left[-m(xt_1-tx_1+yz_1-zy_1)\right]^2.$$

Diese Gleichung läßt sich aber durch m^2 dividieren und wir erhalten schließlich:

7.) $\left[p - (xx_1+yy_1+zz_1+tt_1)\right]^2 + \left[xy_1-yx_1+zt_1-tz_1\right]^2$
$+ \left[xz_1-zx_1-yt_1+ty_1\right]^2 + \left[xt_1-tx_1+yz_1-zy_1\right]^2 = pm_1$.

Durch diese Umformung ist erreicht, daß aus den vier ursprünglich erhaltenen Zahlen x, y, z, t, deren Quadratsumme pm ist, vier neue ganze Zahlen — eben die Klammerausdrücke in 7.) — gebildet werden können, deren Quadratsumme pm_1 ist. Da nun m_1 kleiner als m ist, so hat man hier ein kleineres Vielfaches von p als Quadratsumme dargestellt. Wenn die ganze Zahl m_1 nicht gleich 1 ist, so kann man dies Verfahren solange fortsetzen, bis man endlich vier Zahlen X, Y, Z, T, erhält, deren Quadratsumme gleich p ist:

8.) $X^2 + Y^2 + Z^2 + T^2 = p$.

Dabei brauchen die Zahlen nicht alle verschieden zu sein, auch können einige Null sein. Da nun $2 = 1^2 + 1^2 + 0^2 + 0^2$ ist, so gilt die

[1] Beispiel: $2^2+3^2+4^2+6^2 = 5 \cdot 13$; $x_1 = 0$, $y_1 = z_1 = t_1 = 1$ ergibt $2^2 + (-2)^2 + (-1)^2 + (+1)^2 = 5 \cdot 2$.

Gleichung 8.) auch für die bisher ausgenommene gerade Primzahl 2 und man erhält den Satz:

Jede Primzahl ist als Summe von höchstens vier Quadraten darstellbar.

VI. Jede Zahl läßt sich als Produkt von Primzahlen darstellen. Da aber nach Formel 6.) das Produkt zweier Summen von je vier Quadraten wieder eine solche Summe ist, so gilt der obige Satz auch für jede zusammengesetzte Zahl, d. h.:

Jede ganze Zahl ist als Summe von höchstens vier Quadraten darstellbar.

VII. Beispiele: 1.) Es war
$2^2+3^2+4^2+6^2=5\cdot 13$, $x_1=0_1 y_1=z_1=t_1=1$, $2^2+(-2)^2+(-1)^2+1^2=5\cdot 2$, also wird nach 7.)
$[13-(0+3+4+6)]^2+(2-0+4-6)^2+(2-0-3+6)^2+(2-0+3-4)^2$
$=0^2+0^2+5^2+1^2=2\cdot 13$; $x_2=y_2=0$, $z_2=2$, $t_2=0$: $(13-10)^2$
$+(0-0+0+2)^2+(0-0-0+0)^2+(0-0+0-0)^2=3^2+2^2=13$.[1]

2.) $p=79$. Man berechnet zunächst die 39 quadratischen Reste und findet daraus leicht folgende Gleichungen:

$2^2+32^2-1=13\cdot 79$	$4^2+33^2+1=14\cdot 79$
$4^2+8^2-1=1\cdot 79$	$6^2+11^2+1=2\cdot 79$
$5^2+23^2-1=7\cdot 79$	$9^2+32^2+1=14\cdot 79$
$6^2+26^2-1=9\cdot 79$	$12^2+31^2+1=14\cdot 79$
$7^2+30^2-1=12\cdot 79$	$13^2+15^2+1=5\cdot 79$
$11^2+14^2-1=4\cdot 79$	$14^2+35^2+1=18\cdot 79$
$15^2+31^2-1=15\cdot 79$	$17^2+37^2+1=21\cdot 79$
$18^2+25^2-1=12\cdot 79$	$20^2+28^2+1=15\cdot 79$
$27^2+33^2-1=23\cdot 79$	$21^2+36^2+1=22\cdot 79$
	$23^2+24^2+1=14\cdot 79$

Nimmt man nun aus jeder der beiden Gruppen eine Gleichung, so erhält man als Summe eine Gleichung von der Form 3.); z. B.

$$5^2+12^2+23^2+31^2=21\cdot 79.$$

Hier wählt man $x_1=0$, $y_1=z_1=z_1=t_1=1$ und erhält nach 5.): $5^2+(-9)^2+2^2+10^2=21\cdot 10$ und damit nach 7.): $3^2+6^2+13^2+24^2=79\cdot 10$.

Jetzt nimmt man $x_2=0$, $y_2=z_2=1$, $t_2=2$, erhält nach 5.): $3^2+(-4)^2+3^2+4^2=10\cdot 5$ und nun nach 7.): $12^2+5^2+15^2+(-1)^2=79\cdot 5$.

Wählt man $x_3=2$, $y_3=1$, $z_3=3$, $t_3=0$, so ergibt sich zunächst $2^2+0^2+0^2+(-1)^2=5\cdot 1$; es ist also auch $2^2+0^2+0^2+1^2=5\cdot 1$.

Daraus folgen nach 7.) die beiden Darstellungen:

$$2^2+5^2+5^2+5^2=79 \text{ und } 1^2+2^2+5^2+7^2=79.$$

Durch andere Zusammenstellung erhält man noch $3^2+3^2+5^2+6^2=79$.

3.) $p=31$. Zunächst bildet man die Gleichungen $5^2+6^2+1=31\cdot 2$, $8^2+11^2+1=31\cdot 6$, $12^2+14^2+1=31\cdot 11$; $5^2+10^2-1=31\cdot 4$, $7^2+12^2-1=31\cdot 7$.

[1] Man kann beweisen: Jede Primzahl von der Form $4n+1$ läßt sich als Summe von zwei Quadraten darstellen.

Dann ergeben sich in derselben Weise die Formeln

$$31 = 1^2 + 1^2 + 2^2 + 5^2 = 2^2 + 3^2 + 3^2 + 3^2.$$

4.) Zerlegung von $\mathbf{18142 = 2 \cdot 47 \cdot 193.}$

Man hat $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Für 47 erhält man aus den Resten die Gleichung $3^2 + 4^2 + 15^2 + 19^2 = 47 \cdot 13$, die schließlich $6^2 + 1^2 + 1^2 + 3^2 = 47$ ergibt. Ebenso erhält man aus $4^2 + 5^2 + 16^2 + 19^2 = 47 \cdot 14$ die Gleichung $2^2 + 3^2 + 3^2 + 5^2 = 47$.

Für 193 erhält man sehr schnell die Gleichung $193 = 7^2 + 12^2 + 0^2 + 0^2$.

Multipliziert man nach Formel 6.), so ergeben sich die Resultate:

$$18142 = 4^2 + 49^2 + 62^2 + 109^2 = 2^2 + 31^2 + 61^2 + 116^2 = 14^2 + 24^2 + 87^2 + 99^2.$$