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 $2^2+3^2+4^2+6^2=5\cdot 13$.