Satz 6.8 (Legendre): Seien $a,b,c \in \mathbb{Z}$ verschieden, quadratfrei, paarweise und nicht alle gleichzeitig positiv oder negativ. Die diophantische Gleichung $aX^2+bY^2+cZ^2=0$ hat eine nicht-triviale ganzzahlige Lösung genau dann, wenn

(i) $-ab$ ist ein quadratischer Rest mod $|c|$

(ii) $-ac$ ---------- mod $|b|$

und (iii) $-bc$ ---------- mod $|a|$

wir zeigen erst die Äquivalenz zum Folgenden Satz

Satz 6.9: Seien $a,b \in \mathbb{N}^+$ quadratfrei

$aX^2+bY^2=Z^2$ hat eine nicht-triviale ganzzahlige Lösung genau dann, wenn

(i) a ist eine Quadratzahl mod b

(ii) b ---------- mod a

und (iii) $\frac{ab}{(ggT(a,b))^2}$ ---------- mod $ggT(a,b)$

Bemerkung: von jedem Satz ist die Hinrichtung relativ einfach.

z.B. in Satz 6.8, sei (x,y,z) eine nicht-triviale ganzzahlige Lösung mit $ggT(x,y,z)=1$

Dann gilt $ax^2+by^2=-cz \equiv 0 \mod |c|$

$\Rightarrow ax^2 \equiv -by^2 \mod |c|$

$\Rightarrow (axy^{-1})^2 \equiv -ab \mod |c|$

(y^{-1} existiert da $(c,y)=1$, sonst wäre $(c,y) \mid -z^2 - by^2 = ax^2$

$\Rightarrow (c,y) \mid x$ da $(a,c)=1$, c quadratfrei

$\Rightarrow (c,y)^2 \mid ax^2+by^2=-cz^2$

$\Rightarrow (c,y) \mid z$ ↯ da $ggT(x,y,z)=1$)

$\Rightarrow -ab$ ein quadratischer Rest $\mod |c|$

in Satz 6.9, sei x,y,z eine nicht-triviale ganzzahlige Lösung mit $ggT(x,y,z)$

Dann gilt $g := ggT(a,b) \mid ax^2+by^2=z^2$

$\Rightarrow g \mid z$ da g quadratfrei

$\Rightarrow \frac{a}{g}x^2+\frac{b}{g}y^2=\frac{z^2}{g} \equiv 0 \mod g$

$\Rightarrow \frac{a}{g}x^2 \equiv \frac{-b}{g}y^2 \mod g$

$\Rightarrow \left(\frac{a}{g}xy^{-1}\right) \equiv \frac{-ab}{g^2} \mod g$

(y^{-1} existiert da $(g,y)=1$, sonst wäre $(g,y)^2 \mid z^2 - by^2 = ax^2$

$\Rightarrow (g,y) \mid x^2$ (da a quadratfrei)

$\Rightarrow (g,y) \mid x$ (da g quadratfrei)

↯ da $gg^T(x,y,z)=1$)

$\Rightarrow \frac{-ab}{g^2}$ eine Quadratzahl mod g

Wir müssen also jeweils die Rückrichtung beweisen.

Beweis der Äquivalenz der Sätze 6.8 und 6.9:

6.8 $\Rightarrow$ 6.9: Wende Satz 6.8 mit $c=-1$ an.

6.9 $\Rightarrow$ 6.8: Gegeben die Gleichung $aX^2+bY^2+cZ^2=0$ (1)

sei oBdA $c<0<a,b$

Betrachte die neue Gleichung $(-ca)X^2+(-cb)Y^2 = (-cZ)^2$

$= (Z')^2$ (2)

$-ab$ ein quadratischer Rest mod $|c| \Rightarrow -\frac{(-ac)(-bc)}{c^2}$ ein quadratischer Rest mod $|c|$

$\Rightarrow -\frac{(-ac)(-bc)}{(-ac,-bc)^2}$ ein quadratischer Rest mod $(-ac,-bc)$

$-ac$ ein quadratische Rest mod $|b|$ und eine Quadratzahl ($\equiv 0$) mod $|c|$, also eine Quadratzahl mod $|-bc|$ (da $(b,c)=1$)

ähnlich ist $-bc$ eine Quadratzahl mod $|-ac|$.

Wenn die drei Bedingungen in Satz 6.8 für (1) erfüllt sind, sind auch die Bedingungen in Satz 6.9 für (2) erfüllt.

Und (x', y', z') ist eine Lösung zu (2)

$\Rightarrow (x, y, z) = (-cx', -cy', z')$ ist eine Lösung zu (1). □

Für den Beweis von Satz 6.9 brauchen wir folgende Aussage:

Lemma 6.10: Sei $a \in \mathbb{N}^+$ sodass -1 ein quadratischer Rest mod a.

Dann ist $a = r^2 + s^2$ für $r, s \in \mathbb{N}$

Beweis: (Übungs-) Aufgabe Beobachtung: $\exists x$ sodass $x^2 + 1^2 = an$ für ein $n \in \mathbb{N}$.

Beweis von Satz 6.9:

Für $a=1$ nehmen wir die Lösung $b-1, 2, b+1$
(oder ein beliebiges Pythagoräisches Tripel falls $b=1$)

Ähnlich gilt der Satz falls $b=1$.

Falls $a=b$, ist wegen (iii)

$\frac{-ab}{(ggT(a,b))^2} = -1$ ein quadratischer Rest mod a

$\Rightarrow \exists r,s \in \mathbb{N}$ sodass $r^2+s^2=a=b$ (L 6.10)

und weil a,b quadratfrei (und $\neq 0$) sind, sind $r,s \neq 0$.

Sei dann $x=r$, $y=s$ und $z=r^2+s^2$

Dann ist $ax^2+by^2 = (r^2+s^2)r^2 + (r^2+s^2)s^2$

$= (r^2+s^2)^2$

$= z^2$

und (x,y,z) ist eine nicht-triviale ganzzahlige Lösung.

Also gilt Satz 6.9 falls $a=1$, $b=1$ oder $a=b$

Es sei o.Bd.A $a>b$

Idee: Aus $aX^2+bY^2=Z^2$ (1)

konstruieren wir eine neue Gleichung

$AX^2+bY^2=Z^2$ (2)

sodass (1) eine Lösung hat, wenn (2) eine Lösung hat, und sodass $0<A<a$

Wenden wir diese Konstruktion immer wieder an, (eventuell mit tauschen von A und b falls $A<b$), so reduzieren wir den allgemeinen Fall auf einen der Fälle $a=1$, $b=1$ und $a=b$.

Konstruktion von A

Wegen Bedingung (ii) existieren $c, T \in \mathbb{Z}$ sodass

$$c^2 - b = aT \qquad \text{(wir wählen } c \text{ sodass } |c| \leq \tfrac{a}{2}\text{)}$$

Sei $T = Am^2$ $\quad A, m \in \mathbb{N}$ mit A quadratfrei

↳ wegen $0<b<a$ ist $c^2 - b \geq 0$

weil $b \neq 1$ quadratfrei ist, ist $c^2 - b \neq 0$

Es gilt auch $aAm^2 = c^2 - b < c^2 \leq \frac{a^2}{4}$

$$\Rightarrow \quad A \leq Am^2 < \frac{a}{4} < a$$

Also ist $0 < A < a$

Wir müssen aber wissen, dass A, b die Bedingeungen (i)-(iii) in Satz 6.9 erfüllen.

A ist ein quadratischer Rest mod b:

Sei $d := ggT(a,b)$ und $a = a_1 d$

$b = b_1 d$

Weil a, b quadratfrei sind, ist $(a_1, d) = (b_1, d) = 1$

Es ist $c^2 - b = aAm^2$

$c^2 - b_1 d = a_1 d A m^2$

$\Rightarrow d \mid c^2 \Rightarrow d \mid c$ (d quadratfrei)

$\Rightarrow c = c_1 d \quad (c_1 \in \mathbb{Z})$

$\Rightarrow (c_1 d)^2 - b_1 d = a_1 d A m^2$

$\Rightarrow c_1^2 d - b_1 = a_1 A m^2$

$\Rightarrow -b_1 \equiv a_1 A m^2 \mod d$

da $ggT(b_1, d) = 1$ ist $ggT(a_1 A m^2, d) = 1$

$\Rightarrow (m, d) = 1$

also existieren a_1^{-1} und $m^{-1} \mod d$

$\Rightarrow A \equiv -b_1 a_1^{-1} (m^{-1})^2 \mod d$

$\equiv (a_1^{-1} m^{-1})^2 \cdot (-a_1 b_1) \mod d$

$\equiv (a_1^{-1} m^{-1})^2 \cdot \left(\frac{-ab}{d^2}\right) \mod d$

quadratisch, quadratisch wegen (iii)

$\Rightarrow$ A ein quadratischer Rest mod d.

Ausserdem ist $c^2 - b_1 d = a A m^2$

$$\Rightarrow \quad c^2 \equiv a A m^2 \mod b_1$$

Angenommen $(m, b_1) \neq 1$

$$\Rightarrow (m, b) \neq 1$$

$$c^2 - b = a A m^2 \Rightarrow (m, c) \neq 1$$

und $(m, c)^2 \mid b$ $\lightning$ (b quadratfrei)

Also ist $(m, b_1) = 1$ und $(a, b_1) = 1$

also existieren a^{-1} und $m^{-1} \mod b_1$

$$\Rightarrow A \equiv c^2 a^{-1} (m^{-1})^2 \mod b_1$$

$$\equiv (c a^{-1} m^{-1})^2 a \mod b_1$$

und weil a ein quadratischer Rest mod b ist (Bedingung (i))
ist a ein quadratischer Rest mod b_1

also ist (wegen $b = b_1 d$, $(b_1, d) = 1$) A ein quadratischer Rest mod b.

<u>b ein quadratischer Rest mod A:</u>

$$c^2 - b = a A m^2$$

$$\Rightarrow c^2 \equiv b \mod A$$

$\Rightarrow$ b ein quadratischer Rest mod A.

$-Ab$

$(ggT(A,b))^2$ ein quadratischer Rest mod $ggT(A,b)$:

Sei $e := ggT(A,b)$, $A = A_2 e$

$b = b_2 e$

Es ist $(A_2, b) = 1$

$$c^2 - b_2 e = a A_2 e m^2$$

$\Rightarrow e \mid c^2$

$\rightarrow e \mid c$ (e quadratfrei)

$\Rightarrow -b_2 \equiv a A_2 m^2 \mod e$

$\Rightarrow -A_2 b_2 \equiv a (A_2 m)^2 \mod e$

a ist ein quadratischer Rest mod b

also auch ein quadratischer Rest mod e

$\Rightarrow -A_2 b_2 = \frac{-Ab}{e^2}$ ist ein quadratischer Rest mod e.

Als letztes zeigen wir, dass Gleichung (1) eine nicht-triviale ganzzahlige Lösung hat wenn (2) eine nicht-triviale ganzzahlige Lösung hat.

Sei (x, y, z) eine nicht-triviale ganzzahlige Lösung zu (2) mit $ggT(x,y,z)=1$.

$$Ax^2 + by^2 = z^2 \iff Ax^2 = z^2 - by^2$$

$$\iff aAm^2Ax^2 = (z^2-by^2)(c^2-b)$$

$$\iff a(Amx)^2 = (zc+by)^2 - b(cy+z)^2$$

$$\iff a(Amx)^2 + b(cy+z)^2 = (zc+by)^2$$

Dann ist $(Amx, cy+z, zc+by)$ eine ganzzahlige Lösung zu (1)

Wäre $cy+z=0$, dann ist $ax^2+by^2 = c^2y^2$

$$\Rightarrow ax^2 = (c^2-b)y^2$$

$$= aAm^2y^2$$

$$\Rightarrow x^2 = Am^2y^2$$

$$\Rightarrow A = 1 \quad (A \text{ quadratfrei})$$

aber der Fall war schon gelöst

Wir können y und z auch mit ± 1 multiplizieren, also wählen wir oBdA y, z sodass $zc, by > 0 \Rightarrow zc+by > 0$.

und wir haben schon bewiesen, dass $A, m \neq 0$

also ist diese Lösung nicht-trivial. $\square$