Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 26

Der Reduktionstyp einer elliptischen Kurve

DEFINITION 26.1. Es sei $E = V_+(F)$ eine elliptische Kurve über $\mathbb{Q}$ mit einem homogenen kubischen ganzzahligen Polynom $F \in \mathbb{Z}[X,Y,Z]$ und sei p eine Primzahl. Man sagt, dass E *gute Reduktion* modulo p besitzt, wenn E_p glatt ist, und andernfalls, dass E *schlechte Reduktion* modulo p besitzt.

Da wir mit einer fixierten Gleichung (und nicht mit den sogenannten global minimalen Gleichungen über $\mathbb{Z}$) arbeiten, hängt das Reduktionsverhalten nicht nur von der elliptischen Kurve über $\mathbb{Q}$, sondern von der Gleichung selbst ab. So gesehen sind diese Eigenschaften keine Eigenschaften der Kurve über $\mathbb{Q}$, sondern der (relativen) Kurve über $\mathbb{Z}$.

BEISPIEL 26.2. Die elliptische Kurve E zur Fermatkubik

$$X^3+Y^3+1$$

besitzt für alle Primzahlen $p \neq 3$ nach Lemma 4.7 gute Reduktion und bei $p = 3$ ist wegen

$$(X+Y+1)^3 = X^3+Y^3+1$$

die Kurve E_3 eine nichtreduzierte Kurve und insbesondere in jedem Punkt singulär. Geometrisch ist es die durch $X+Y+1 = 0$ gegebene Gerade, aber mit einer verdickten algebraischen Struktur.

Im Fall von schlechter Reduktion sind weitere Unterscheidungen nötig, je nachdem, was für Singularitäten auftreten.

Zumeist betrachtet man ganzzahlige Weierstraßgleichungen für die elliptische Kurve, bei denen der Koeffizient zu Y^2 und zu X^3 gleich 1 ist. Dies sichert nach Aufgabe 25.2, dass die Kurve modulo p irreduzibel bleibt. In diesem Fall kann nur ein einzelner singulärer Punkt auftreten, und zwar ist dieser singuläre Punkt schon über $\mathbb{Z}/(p)$ sichtbar (und nicht erst über einer endlichen Erweiterung $\mathbb{F}_{p^e}$).

Für diesen singulären Punkt gibt es dann zwei Möglichkeiten, nämlich, ob eine Spitze (Kuspe) oder ob ein Überkreuzungspunkt auftritt. Im letzteren Fall können die Tangenten in diesem Punkt über $\mathbb{Z}/(p)$ definiert sein oder erst in einer endlichen Erweiterung von $\mathbb{Z}/(p)$.

Wir erinnern kurz an das Konzept einer Tangente in einem singulären Punkt.

Es sei K ein Körper und sei $F \in K[X,Y]$ ein von 0 verschiedenes Polynom. Es sei $P = (x,y) \in C = V(F) \subset \mathbb{A}^2_K$ ein Punkt der zugehörigen affinen ebenen Kurve. Indem man F in den verschobenen Variablen $U = X - x$, $V = Y - y$ schreibt, so erhält man ein neues Polynom H mit $H(0,0) = 0$. Es sei

$$H = H_m + H_{m+1} + \cdots + H_d$$

die homogene Zerlegung von H mit $H_m \neq 0$ und $H_d \neq 0$, $d \geq m$. Dabei ist d der Grad der Kurve und m heißt die *Multiplizität* der Kurve im Punkt P. Die Kurve besitzt genau dann eine Singularität in P, wenn $m \geq 2$ ist. Bei einer Faktorzerlegung $H_m = G_1 \cdots G_m$ in lineare Faktoren, die eventuell erst nach einer endlichen Körpererweiterung vorliegt, nennt man die Geraden $V(G_i)$, $i = 1, \ldots, m$, die *Tangenten* an C im Punkt P. Im kubischen Fall ist in einem singulären Punkt $2 \leq m \leq 3$, wobei bei $m = 3$ keine irreduzible Kurve vorliegt. Im irreduziblen Fall ist $2 = m$ und dort gibt es eine Faktorzerlegung $H_2 = G_1 G_2$, wobei die beiden Faktoren gleich oder verschieden sein können.

Definition 26.3. Es sei $E = V_+(F)$ eine elliptische Kurve über $\mathbb{Q}$ mit $F \in \mathbb{Z}[X,Y,Z]$ und sei p eine Primzahl. Man sagt, dass E *additive Reduktion* modulo p besitzt, wenn E_p irreduzibel ist und einen singulären Punkt mit einer Tangentenrichtung besitzt.

Im Fall von additiver Reduktion liegt (affin) im Wesentlichen eine Neilsche Parabel $Y^2 = X^3$ vor.

Definition 26.4. Es sei $E = V_+(F)$ eine elliptische Kurve über $\mathbb{Q}$ mit $F \in \mathbb{Z}[X,Y,Z]$ und sei p eine Primzahl. Man sagt, dass E *multiplikative Reduktion* modulo p besitzt, wenn E_p irreduzibel ist und einen singulären Punkt mit zwei Tangentenrichtungen besitzt.

Man beachte, dass die Tangentenrichtungen erst nach einer endlichen Erweiterung des Körpers sichtbar werden können. Diese Sprechweisen haben folgenden Hintergrund: Im singulären Fall liegt keine Gruppenstruktur auf der Kurve mehr vor. Allerdings gibt es eine Gruppenstruktur außerhalb des singulären Punktes. Wenn die Singularität eine Kuspe ist, so ist das Komplement isomorph zur affinen Geraden mit der additiven Struktur, siehe Aufgabe 26.10. Wenn die Singularität ein Kreuzungspunkt ist, so ist das Komplement eine punktierte affine Gerade (man denke an die Normalisierung der Kurve, wo ja zwei Punkte oberhalb des singulären Punktes liegen) und isomorph zur multiplikativen Gruppe $(\mathbb{A}^1_K \setminus \{0\}, \cdot, 1)$.

Definition 26.5. Es sei $E = V_+(F)$ eine elliptische Kurve über $\mathbb{Q}$ mit $F \in \mathbb{Z}[X,Y,Z]$ und sei p eine Primzahl. Man sagt, dass E *spaltende multiplikative Reduktion* modulo p besitzt, wenn E_p irreduzibel ist und einen singulären Punkt mit zwei Tangentenrichtungen besitzt, die über $\mathbb{Z}/(p)$ definiert sind.

Andernfalls spricht man von nichtspaltender multiplikativer Reduktion.

Beispiel 26.6. Wir betrachten die elliptische Kurve E, die durch die affine Gleichung

$$Y^2 = X^3 + 1$$

gegeben ist. Die partiellen Ableitungen sind

$$2Y \text{ und } 3X^2 .$$

Bei $p \neq 2, 3$ verschwinden die beiden partiellen Ableitungen nur im Punkt $(0, 0)$, doch dies ist kein Punkt der Kurve. Für $p \geq 5$ ist die Kurve E_p also glatt und es liegt gute Reduktion vor. Bei $p = 2$ liegt in $(0, 1)$ ein singulärer Punkt der Kurve vor. In den lokalen Koordinaten $(X, Y - 1)$ wird das beschreibende Polynom zu $(Y - 1)^2 - X^3$. Das ist eine Neilsche Parabel und es liegt eine Kuspe, also additive Reduktion vor. Bei $p = 3$ liegt in $(-1, 0)$ ein singulärer Punkt der Kurve vor. In den lokalen Koordinaten $(X + 1, Y)$ wird das beschreibende Polynom zu $Y^2 - (X + 1)^3$. Das ist wieder eine Neilsche Parabel und es liegt wieder additive Reduktion vor.

Beispiel 26.7. Wir betrachten die elliptische Kurve E, die durch die affine Gleichung

$$Y^2 = X^3 - X = X(X - 1)(X + 1)$$

gegeben ist. Die partiellen Ableitungen sind

$$2Y \text{ und } 3X^2 - 1 .$$

Bei $p \neq 2$ verschwindet die erste partielle Ableitung nur bei $Y = 0$. Wegen der Kurvengleichung ist dann $X = 0, 1, -1$ doch dann verschwindet die zweite partielle Ableitung nicht. Für $p \geq 3$ ist die Kurve E_p also glatt und es liegt gute Reduktion vor. Bei $p = 2$ liegt in $(1, 0)$ ein singulärer Punkt der Kurve vor. In den lokalen Koordinaten $(X - 1, Y)$ wird das beschreibende Polynom zu $Y^2 + (X + 1)^3 + (X + 1)^2$. Wir schreiben dies mit $W = X + 1$ als

$$Y^2 + (X + 1)^3 + (X + 1)^2 = Y^2 + W^3 + W^2 = (Y + W)^2 + W^3$$

und somit ist dies eine Neilsche Parabel. Es liegt also additive Reduktion vor.

Beispiel 26.8. Es sei p eine Primzahl. Wir betrachten die elliptische Kurve E, die durch die affine Gleichung

$$Y^2 = X(X - 1)(X - p) = X^3 - (p + 1)X^2 + pX$$

gegeben ist. In Charakteristik p ist $(0, 0)$ ein singulärer Punkt der Kurve, die Gleichung wird zu

$$Y^2 = X^3 - X^2$$

bzw. zu

$$X^2 + Y^2 - X^3 = 0.$$

Bei $p \geq 3$ gilt für den quadratischen Term

$$X^2 + Y^2 = (X + \mathrm{i}Y)(X - \mathrm{i}Y),$$

wobei i $\in \overline{\mathbb{Z}/(p)}$ eine Quadratwurzel aus -1 sei. Diese beiden lineare Terme sind verschieden und beschreiben die verschiedenen Tangenten, es liegt also multiplikative Reduktion vor. Das Spaltungsverhalten hängt davon ab, ob die -1 in $\mathbb{Z}/(p)$ eine Quadratwurzel besitzt oder erst in einer endlichen Erweiterung (und zwar dann in $\mathbb{F}_{p^2}$). Nach Satz 6.8 (Zahlentheorie (Osnabrück 2016-2017)) besitzt -1 eine Quadratwurzel in $\mathbb{Z}/(p)$ genau dann, wenn $p = 1$ mod 4 ist. Unter dieser Bedingung liegt also modulo p spaltender multiplikativer Typ vor und andernfalls nichtspaltender multiplikativer Typ.

Die L-Reihe einer elliptischen Kurve

Es sei E eine elliptische Kurve über $\mathbb{Q}$, gegeben in ganzzahliger Darstellung. Für fast alle Primzahlen p ist dann E_p modulo p eine elliptische Kurve über $\mathbb{Z}/(p)$. Es sei N_p die Anzahl der $\mathbb{Z}/(p)$-Punkte von E_p, die ja endlich ist. Aufgrund der Abschätzung von Hasse erwartet man eine Größenordnung von $p+1$. Es fällt einem zunächst mal kein Grund ein, warum die Zahlen N_p zu verschiedenen Primzahlen etwas miteinander zu tun haben sollten. Deshalb packt man diese Daten in eine L-Reihe und hofft, dass sich dadurch Gesetzmäßigkeiten ergeben (bzw. dieser Zugang ist sinnvoll, weil dadurch Gesetzmäßigkeiten sichtbar werden). Statt mit N_p direkt arbeitet man mit $p+1-N_p$, da diese Terme um 0 schwanken. Für Primzahlen mit schlechter Reduktion müssen besondere Festlegungen getroffen werden.

Definition 26.9. Zu einer elliptischen Kurve E über $\mathbb{Q}$ in ganzzahliger Darstellung und einer Primzahl p definiert man

$$a_p = \begin{cases} p+1-\#\left(E_p(\mathbb{Z}/(p)\right), \text{ wenn } E \text{ gute Reduktion modulo } p \text{ besitzt}, \\ 1, \text{ wenn } E \text{ spaltende multiplikative Reduktion modulo } p \text{ besitzt}, \\ -1, \text{ wenn } E \text{ nichtspaltende multiplikative Reduktion modulo } p \text{ besitzt}, \\ 0, \text{ wenn } E \text{ additive Reduktion modulo } p \text{ besitzt}. \end{cases}$$

Definition 26.10. Zu einer elliptischen Kurve E über $\mathbb{Q}$ in ganzzahliger Darstellung und einer Primzahlpotenz p^r definiert man unter Verwendung von $a_1 = 1$ und der Definition 26.9 von a_p rekursiv

$$a_{p^{r+1}} = \begin{cases} a_p \cdot a_{p^r} - p \cdot a_{p^{r-1}}, \text{ wenn } E \text{ gute Reduktion modulo } p \text{ besitzt}, \\ a_p^{r+1}, \text{ wenn } E \text{ schlechte Reduktion modulo } p \text{ besitzt}. \end{cases}$$

Nach Aufgabe 23.9 erfüllen bei guter Reduktion die Zahlen $b_{p^r} := p^r + 1 - E_p(\mathbb{F}_{p^r})$ ebenfalls diese rekursive Relation, allerdings erst für $r \geq 3$, für $r = 2$ gilt dort $b_{p^2} = b_p b_p - 2p$.

Definition 26.11. Zu einer elliptischen Kurve E über $\mathbb{Q}$ in ganzzahliger Darstellung und einer natürlichen Zahl $n = p_1^{r_1} \cdots p_k^{r_k}$ setzt man unter Verwendung der Definition 26.10

$$a_n = a_{p_1^{r_1}} \cdots a_{p_k^{r_k}}.$$

Definition 26.12. Zu einer elliptischen Kurve E über $\mathbb{Q}$ in ganzzahliger Darstellung definiert man die *L- Reihe* unter Verwendung der Definition 26.11 durch

$$L(E,s) = \sum_{n \in \mathbb{N}_+} a_n n^{-s}.$$

Reihen von dieser Bauart nennt man Dirichletreihen, man fasst sie als Funktion in der einen komplexen Variablen s auf, wobei das Konvergenzverhalten von den Koeffizienten abhängt. Die bekannteste Reihe von dieser Form ist die Riemannsche ζ-Funktion, die durch

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

gegeben sind, dort sind also sämtliche Koeffizienten gleich 1.

Für die Riemannsche ζ-Funktion gilt

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}}$$

nach Satz 11.5 (Zahlentheorie (Osnabrück 2016-2017)). Ebenso besitzt die L-Reihe zu einer elliptischen Kurve E neben der additiven Darstellung auch eine multiplikative Darstellung, bei der die Weilschen Zeta-Funktionen zu E_p eine wichtige Rolle spielen. Gemäß Satz 24.4 gilt im Falle guter Reduktion

$$Z(E_p;t) = \frac{1+(N_1-p-1)t+pt^2}{(1-t)(1-pt)} = \frac{1-a_pt+pt^2}{(1-t)(1-pt)},$$

d.h. das a_p beschreibt vollständig die Zeta-Funktion der Reduktion E_p. Wenn man in die obige Zeta-Funktion $t = p^{-s}$ einsetzt, so erhält man

$$\begin{aligned} Z(E_p;p^{-s}) &= \frac{1+(N_1-p-1)p^{-s}+pp^{-2s}}{(1-p^{-s})(1-pp^{-s})} \\ &= \frac{1+(N_1-p-1)p^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} \\ &= \frac{1-a_pp^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}. \end{aligned}$$

Wenn man versucht, darüber das Produkt über alle Primzahlen p zu bilden, so fällt zunächst auf, dass das Produkt über den linken Faktor im Nenner $\zeta(s)$ ergibt und dass das Produkt über den rechten Faktor $\zeta(s-1)$ ergibt. Man kann sich also auf den Zähler konzentrieren.

Die folgende Aussage beschreibt die multiplikative Version der L-Reihe.

Lemma 26.13. *Für eine über $\mathbb{Z}$ definierte elliptische Kurve E gilt für die L-Reihe für* $\operatorname{Re}(s) > 1$ *die Produktdarstellung*

$$L(E,s) = \prod_{p \text{ schlechte Reduktion}} \frac{1}{1-a_pp^{-s}} \cdot \prod_{p \text{ gute Reduktion}} \frac{1}{1-a_pp^{-s}+p^{1-2s}}.$$

Beweis. Aufgrund von Definition 26.11 sind die Koeffizienten der L-Reihe

$$L(E,s) = \sum_{n \in \mathbb{N}_+} a_n n^{-s}$$

multiplikativ, daher gibt es nach Lemma Anhang 7.8 eine Produktdarstellung $L(E,s) = F_p(s)$ mit den lokalen Faktoren

$$F_p(s) = \sum_{k \in \mathbb{N}} a_{p^k} p^{-ks}.$$

Wir müssen zeigen, dass diese Faktoren mit den im Satz formulierten Faktoren in den beiden Fällen übereinstimmen.

Bei guter Reduktion wird

$$F_p(s) = \sum_{k \in \mathbb{N}} a_{p^k} p^{-ks} = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

behauptet. Wir schreiben den letzten Bruch unter Verwendung von Satz 9.13 (Analysis (Osnabrück 2021-2023)) als geometrische Reihe, es ist also

$$\frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{\ell=0}^{\infty} \left(a_p p^{-s} - p^{1-2s}\right)^{\ell} = \sum_{\ell=0}^{\infty} \left(a_p - p \cdot p^{-s}\right)^{\ell} p^{-s\ell}.$$

Wenn man hier (siehe Aufgabe 26.15 mit $t = p^{-s}$) die Terme zusammenfasst, die sich auf p^{-sk} beziehen, so erhält man Koeffizienten, die die Anfangsbedingungen und die rekursiven Bedingungen erfüllen, also mit den Koeffizienten aus den Definitionen übereinstimmen.

Der Fall von schlechter Reduktion folgt direkt aus der geometrischen Reihe. □

Wenn man die Zeta-Funktion für die Primzahlen mit schlechter Reduktion als

$$Z(E_p;t) := \frac{1 - a_p t}{(1-t)(1-pt)}$$

bzw.

$$Z(E_p;p^{-s}) := \frac{1 - a_p p^{-s}}{(1-p^{-s})(1-pp^{-s})}$$

ansetzt, so erhält man die Darstellung

$$\begin{aligned} & L(E,s) \\ = & \prod_{p \text{ schlechte Reduktion}} \frac{1}{1 - a_p p^{-s}} \cdot \prod_{p \text{ gute Reduktion}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \\ = & \prod_{p \text{ schlechte Reduktion}} \frac{1}{(1-p^{-s})(1-p^{1-s})Z(E_p;p^{-s})} \\ & \cdot \prod_{p \text{ gute Reduktion}} \frac{1}{(1-p^{-s})(1-p^{1-s})Z(E_p;p^{-s})} \end{aligned}$$

$$= \prod_p \frac{1}{1-p^{-s}} \prod_p \frac{1}{1-p^{1-s}} \prod_p \frac{1}{Z(E_p;p^{-s})} = \zeta(s)\zeta(s-1) \prod_p \frac{1}{Z(E_p;p^{-s})},$$

und die L-Reihe ergibt sich bis auf die zwei Vorfaktoren, die von der Riemannschen Zetafunktion herkommen, als ein Produkt von invertierten Zetafunktionen.

Die Vermutung von Birch und Swinnerton-Dyer

BEMERKUNG 26.14. Es sei E eine elliptische Kurve über $\mathbb{Q}$ und sei $L(E,s)$ die L-Reihe zu E. Die Vermutung von Birch und Swinnerton-Dyer besagt, dass die Nullstellenordnung von $L(E,s)$ in $s=1$ (was voraussetzt, dass es eine holomorphe Fortsetzung in diesen Punkt gibt, siehe Satz 28.6) mit dem Rang von E übereinstimmt. Die Nullstellenordnung nennt man auch den *analytischen Rang* der elliptischen Kurve, so geht es bei der Vermutung also darum, dass der (gruppentheoretische) Rang mit dem analytischen Rang übereinstimmt. Dieses Problem gehört zu den sogenannten Milleniumsproblemen. Es ist bekannt (Ergebnisse von Kolyvagin, Gross, Zagier), dass wenn der analytische Rang gleich 0 ist (die L-Funktion also keine Nullstelle in $s=1$ besitzt), dass dann der Rang gleich 0 ist, und dass, wenn der analytische Rang gleich 1 ist, dann auch der Rang gleich 1 ist.

Ein Spezialfall dieser Vermutung ist die Behauptung, dass L genau dann eine Nullstelle in $s=1$ besitzt, wenn der Rang ≥ 1 ist, was äquivalent dazu ist, dass E unendlich viele rationale Punkte besitzt. Davon ist die Rückrichtung bekannt.

BEMERKUNG 26.15. Eine heuristische Überlegung, die zumindest einen Zusammenhang zwischen einem positiven gruppentheoretischen Rang und einem positiven analytischen Rang vorstellbar macht, geht folgendermaßen. Die durch ganzzahlige Koeffizienten gegebene elliptische Kurve E besitze einen positiven Gruppenrang, also neben der Torsion eine $\mathbb{Z}$-Komponente. Unter der Reduktionsabbildung, siehe Lemma 25.1 und Korollar 25.5, wird $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$ auf die endliche Gruppe $E(\mathbb{Z}/(p))$ abgebildet. Die Anzahl von $E(\mathbb{Z}/(p))$ ist nach Satz 23.10 in der Größenordnung von $p+1$ mit einer Abweichung von maximal $2\sqrt{p}$. Grundsätzlich gibt es keine Tendenz, ob die Anzahl sich eher oberhalb von $p+1$ oder eher unterhalb davon befindet. Bei $r \geq 1$ kann man sich aber vorstellen, dass das Bild von $\mathbb{Z}^r$ tendenziell dazu führt, dass die Anzahlen sich eher oberhalb von $p+1$ bewegen. Wenn wir die Produktdarstellung für $s=1$ anschauen, so sind die Faktoren (es kommt nicht auf die endlich vielen Faktoren zu den Primzahlen mit schlechter Reduktion an) gleich

$$\frac{1}{1-a_p p^{-1}+p^{-1}} = \frac{p}{p-a_p+1} = \frac{p}{\#\left(E_p(\mathbb{Z}/(p))\right)}.$$

Wenn hier die Nenner tendenziell größer als $p+1$ sind, so sind die Faktoren tendenziell „deutlich“ kleiner als 1, was im unendlichen Produkt zu einer (höheren) Nullstelle führen könnte.

Unter der Bedingung, dass die Vermutung von Birch und Swinnerton-Dyer stimmt, hat Tunnell eine überprüfbare Bedingung dafür angegeben, dass eine natürliche Zahl eine kongruente Zahl ist.

Satz 26.16. *Es sei n eine ungerade quadratfreie natürliche Zahl. Es sei vorausgesetzt, dass die Vermutung von Birch und Swinnerten-Dyer stimmt. Dann sind die folgenden Aussagen äquivalent.*

(1) *n ist eine kongruente Zahl.*
(2) *Es gilt*

$$\begin{aligned} & \#\left(\left\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+8z^2=n\right\}\right) \\ = \; & 2\cdot\#\left(\left\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+32z^2=n\right\}\right). \end{aligned}$$

Beweis. Wegen Satz 25.10 wissen wir, dass eine kongruente Zahl genau dann vorliegt, wenn die zugehörige elliptische Kurve einen positiven Rang besitzt. Unter der Vermutung von Birch und Swinnerton-Dyer ist dies genau dann der Fall, wenn der analytische Rang positiv ist, d.h. die zugehörige L-Reihe eine Nullstelle für $s=1$ besitzt. Dies führt dann über weitere schwierige Sätze zu der angegebenen Anzahlbedingung. □

Satz 26.17. *Es sei n eine gerade quadratfreie natürliche Zahl. Es sei vorausgesetzt, dass die Vermutung von Birch und Swinnerten-Dyer stimmt. Dann sind die folgenden Aussagen äquivalent.*

(1) *n ist eine kongruente Zahl.*
(2) *Es gilt*

$$\begin{aligned} & \#\left(\left\{(x,y,z)\in\mathbb{Z}^3 \mid 4x^2+y^2+8z^2=\frac{n}{2}\right\}\right) \\ = \; & 2\cdot\#\left(\left\{(x,y,z)\in\mathbb{Z}^3 \mid 4x^2+y^2+32z^2=\frac{n}{2}\right\}\right). \end{aligned}$$

Dabei ist die Hinrichtung bekannt und unabhängig von der Vermutung von Birch und Swinnerton-Dyer, für die Rückrichtung genügt die schwache Version, und auch die nur für die für kongruente Zahlen relevanten elliptischen Kurven.

Das Entscheidende bei diesen Anzahlbedingungen für kongruente Zahlen ist, dass sie einfach und effektiv überprüfbar sind. Da nur Quadrate vorkommen, sind die möglichen Summanden auf beiden Seiten beschränkt und können somit durchprobiert werden. Schauen wir auf den ungeraden Fall: Bei der nicht kongruenten Zahl 1 sind beide Anzahlen gleich 2, bei der nicht kongruenten Zahl 3 sind beide Anzahlen gleich 4, in diesen Fällen stimmt die Bedingung nicht, bei der kongruenten Zahl 5 sind beide Anzahlen gleich 0 und die Bedingung stimmt. Interessant wird die Bedingung, wenn $n \geq 32$

ist. Für $n = 41$ liegt erstmals eine kongruente Zahl vor, wo beide Mengen nicht leer sind, siehe Aufgabe 26.20.

Abbildungsverzeichnis