Lösungen von $z^4 = x^4 + y^4 + w^4$

Jana Göken, Aimeric Malter

Inhaltsverzeichnis

1 Projektplan

Im Zuge dieses Projektes möchten wir untersuchen und nachvollziehen, wie die Gleichung

$$z^4 = x^4 + y^4 + w^4 \tag{1}$$

von Ph.D. Don Zagier gelöst wurde, zumal hierzu nicht-triviale Methoden angewandt wurden.[1] Diese wollen wir nachvollziehen und überprüfen, inwiefern man sie weiter anwenden kann um andere Gleichungen der Form $x_0^n = x_1^n + x_2^n + \cdots + x_{f(n)}^n$ zu lösen. Hierbei sei $f(n)$ diejenige Funktion, welche die minimale Anzahl an n-ten Potenzen beschreibt, welche benötigt werden um eine n-te Potenz nicht-trivial als Summe darzustellen. Der große Satz von Fermat besagt, dass $f(n) > 2$ für $n \geq 3$ ist.

Insbesondere interessiert uns ob $f(n)$ monoton sein kann. Dies wollen wir prüfen, indem wir nach Lösungen von $x^{2^k} = y^{2^k} + z^{2^k} + w^{2^k}$ suchen.

Es folgt eine sinnhafte Überarbeitung des Papers. In dieser füllen wir die angebrochenen Gedankengänge des Autors aus.

2 Einleitung

Die diophantische Gleichung (1) ist deshalb so interessant, weil sie Teil einer Vermutung Eulers war, die ein Viertel Jahrtausend bestand bis sie widerlegt wurde. Er behauptete, dass die n-te Potenz einer positiven ganzen Zahl niemals als eine Summe von weniger als n anderen n-ten Potenzen positiver ganzer Zahl geschrieben werden könne. Demnach hätte die Gleichung

$$x_1^n = x_2^n + \cdots + x_n^n \tag{2}$$

keine nicht-trivialen Lösungen für nicht-negative ganze Zahlen. Diese Vermutung blieb ungelöst bis 1966, als das Gegenbeispiel

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5 \tag{3}$$

fr $n = 5$ per direkter Computersuche gefunden wurde. Aber der leichter scheinende Fall $n = 4$ blieb für viele weitere Jahre offen.

Bei genauerer Betrachtung jedoch ist die Vermutung Eulers wahrscheinlich für jedes n falsch, wie ein simples Wahrscheinlichkeitsargument zeigt.

[1] Gemeint sind nicht-negative und nicht-triviale Lösungen.

Man betrachte alle n-Tupel $(x_1 \ldots, x_n)$ positiver ganzer Zahlen, für die x_1 genau k Dezimalstellen hat und für die jedes andere x_i ist kleiner ist als x_1. Die Anzahl aller solcher n-Tupel liegt in der Größenordnung 10^{nk}, wobei nk die Anzahl aller Dezimalstellen beschreibt, die alle eine der 10 Ziffern repräsentieren. Da man allerdings noch einige Möglichkeiten entfernen muss, da x_1 die größte Zahl sein muss, keine Null als erste Dezimalstelle haben darf und mindestens 2 weitere Zahlen nicht nur aus Nullen bestehen dürfen, sind es nicht genau 10^{nk} mögliche Tupel. Genauer erhalten wir einen Wert zwischen $c_1 \cdot 10^{nk}$ und $c_2 \cdot 10^{nk}$ fr Konstanten $c_2 > c_1 > 0$.

Fr jedes dieser n-Tupel liegt die Differenz $x_1^n - x_2^n - \cdots - x_n^n$ im Intervall $[-(n-2) \cdot 10^{nk}, 10^{nk}]$. Die obere Grenze, 10^{nk}, kommt zustande, indem man das größte x_1^n und die kleinsten x_i^n benutzt. Für die x_i nehme man also fast ausschlielich Nullen und x_1 bestehe aus k Neunen , was $10^k - 1$, und, unter Vernachlässigung der -1, als n-te Potenz 10^{nk} entspricht. Den kleinstmöglichen Wert der Differenz nähern wir durch $10^{nk}(n-1) \cdot 10^{nk} = -(n-2) \cdot 10^{nk}$ an, da man möglichst große x_i wählen muss, x_1 aber immer noch die größte Zahl sein muss, was zu einem Wert um 10^k fr jedes x_i fhrt. Die Länge dieses Intervalls ist also in der Größenordnung von $n \cdot 10^{nk}$. Zumal jedoch dies nur eine Abschätzung ist gehe man von einem Faktor aus, der von n abhängt.

Teilen wir nun die Anzahl der n-Tupel durch die Anzahl der möglichen Differenzen, erhalten wir die Wahrscheinlichkeit, dass ein Tupel eine bestimmte Differenz ergibt, zum Beispiel Null. Dies wäre eine dann eine Lösung der Gleichung (2). Wir erhalten eine positive Zahl p, die von n, aber nicht von k abhängig ist. Somit haben wir also fr jedes k eine positive Wahrscheinlichkeit, dass die Differenz Null ist und wir eine Lösung fr Gleichung (2) gefunden haben. Lassen wir k gegen unendlich streben, so sehen wir dass die Anzahl der erwarteten Lösungen von (2) gegen unendlich strebt. Allerdings wächst die Anzahl der Lösungen mit weniger als K Stellen sehr langsam, weshalb die Lösungen nicht leicht zu raten sein werden.

3 Das Herangehen an die Gleichung

Die Grundidee mit der man die Gleichung lösen möchte ist es, einen der drei Summanden lediglich als Quadrat zu behandeln. Gesucht sind also Lösungen der Gleichung:

$$z^4 = x^4 + y^4 + t^2. \tag{4}$$

Man versuche nun von dieser Gleichung (4) möglichst viele Lösungen zu finden und dann diejenigen auszusortieren, für die das t selbst ein Quadrat w^2 sein könnte. Bereits 1895 fand Escott eine parametrische Lösung zu (4), nämlich

$$(x^2 + x + 1)^4 = x^4 + (x + 1)^4 + (x^4 + 2x^3 + 3x^2 + 2x)^2 \tag{5}$$

Diese Gleichung kann man in eine homogene Form bringen, sodass die Lösungen für z, x, y, t die Form $\sum_{i+j=c} a_{i,j} u^i v^j$ haben, wobei $a_{i,j} \in \mathbb{R}$ und c konstant ist. Diese Lösung sähe dann so aus: $z = u^2 + uv + v^2$, $x = uv$, $y = uv + v^2$ und $t = u^4 + 2u^3v + 3u^2v^2 + 2uv^3$. In Zukunft kürzen wir die homogene Form ab, indem wir nur noch die Koeffizienten der Reihe nach aufschreiben. So wäre $z = [1, 1, 1], x = [0, 1, 0], y = [0, 1, 1]$ und $t = [1, 2, 3, 2, 0]$. Tatsächlich führt diese spezielle Lösung von (4) niemals zu einer Lösung von (1), da die Diophantische Gleichung

$$w^2 = x^4 + 2x^3 + 3x^2 + 2x$$

keine nicht-trivialen rationalen Lösungen hat.

Beweis. Um dies zu zeigen formen wir die Gleichung ein wenig um:

$$\begin{aligned}
&w^2 = x^4 + 2x^3 + 3x^2 + 2x \quad &&| \div x^4 \\
&\frac{w^2}{x^4} = 1 + \frac{2}{x} + \frac{3}{x^2} + \frac{2}{x^3} \quad &&| \text{ faktorisieren} \\
&\left(\frac{w}{x^2}\right)^2 = \left(\frac{1}{x} + 1\right) \cdot \left(2 \cdot \left(\frac{1}{x}\right)^2 + \frac{1}{x} + 1\right) \quad &&| \ \eta = \frac{w}{x^2}, \xi = \frac{1}{x} \\
&\eta^2 = (\xi + 1)(2\xi^2 + \xi + 1)
\end{aligned}$$

Diese Gleichung beschreibt nun eine elliptische Kurve E über $\mathbb{Q}$. Man betrachte den Punkt $P = (0, 1)$. Jener erfüllt die Gleichung der elliptischen Kurve ($1^2 = (0 + 1)(2 \cdot 0^2 + 0 + 1) = 1$) und liegt mithin auf E. Er hat die Ordnung 4, was bedeutet dass $P + P + P + P = \mathcal{O}$. $\mathcal{O}$ ist hierbei der unendlich ferne Punkt welcher aus der projektiven Geometrie bekannt ist und als neutrales Element der durch einer elliptischen Kurve definierten abelschen Gruppe gilt. Eine Veranschaulichung der Tatsache, dass $4P = \mathcal{O}$ findet sich

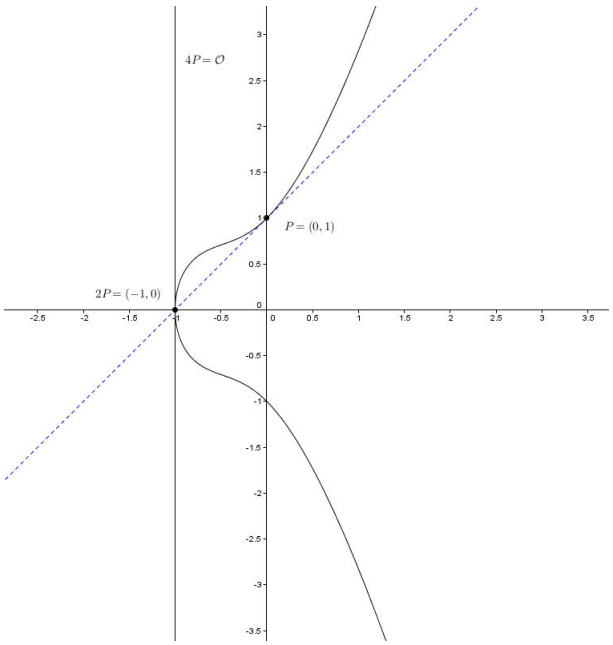

Abbildung 1: Darstellung von $4P = \mathcal{O}$

in Abbildung 1. Jede Lösung von E hat die Eigenschaft, dass entweder $\xi + 1$ ein Quadrat ist (was ab jetzt abgekürzt wird mit $= \square$), oder dass $\xi + 1 = 2 \cdot \square$, da $(\xi + 1)$ und $(2\xi^2 + \xi + 1)$ höchstens den Teiler 2 gemeinsam haben. Somit hat jede rationale Lösung die Form $2Q$ oder $2Q + P$ für ein $Q \in E(\mathbb{Q})$, da eben jene Punkte die gesuchte Eigenschaft erfüllen. Daher ist $E(\mathbb{Q})/2E(\mathbb{Q})$ injektiv in $\mathbb{Z}/2\mathbb{Z}$, denn die Lösungen können zwei verschiedene Formen haben und sind somit injektiv zu den Restklassen der ganzen Zahlen modulo 2. Mithin ist der Rang von E 0, da der Rang einer Kurve beschreibt, wieviele Abbildungen von $\mathbb{Z}$ in ihr zu finden sind. Da jedoch eine injektive Abbildung von E in $\mathbb{Z}/2\mathbb{Z}$ besteht, ist dieser Rang 0.

Somit ist $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Denn dem Satz von Mordell-Weil zufolge ist $E(\mathbb{Q}) \cong Z^{Rang} \oplus E(\mathbb{Q})_{tors}$. $E(\mathbb{Q})_{tors}$ ist hierbei die Torsionsgruppe von $E(\mathbb{Q})$, also die Untergruppe von $E(\mathbb{Q})$ aller Punkte endlicher Ordnung. Insbesondere folgt hieraus, dass $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors}$. Da $E(\mathbb{Q})/2E(\mathbb{Q})$ nun also injektiv in $\mathbb{Z}/2\mathbb{Z}$ ist, muss $r = 0$ gelten.

Wie wir wissen ist diese Gruppe $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$, da wir 4 Punkte endlicher Ordnung haben: $P, 2P, 3P$ und $4P$. Da nach Satz von Mazur nur $\mathbb{Z}/nZ$ mit $1 \leq n \leq 10$ oder $n = 12$ sowie $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ mit $1 \leq n \leq 4$

mögliche Torsionsgruppen sind, müsste es, damit $E(\mathbb{Q})_{tors} \ncong \mathbb{Z}/4\mathbb{Z}$ gelten könnte, noch mindestens einen nicht in $\{P, 2P, 3P, \mathcal{O}\}$ enthaltenen Punkt mit Ordnung 2 geben. Aufgrund der Konstruktion jedoch ist dies nicht möglich[2]. Und da somit $E(\mathbb{Q})_{tors}$ nicht $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ sein kann, ist $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$.

Zumal jetzt der Rang von $E = 0$ ist, ist also $E(\mathbb{Q}) \cong \mathbb{Z}^0 \oplus \mathbb{Z}/4\mathbb{Z} = \emptyset \oplus \mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$. Die Mächtigkeit von $E(\mathbb{Q})$ ist somit gleich der von $\mathbb{Z}/4\mathbb{Z}$, nämlich 4. Jedoch kennen wir mit $P, 2P, 3P$ und $4P = \mathcal{O}$ vier rationale Punkte auf der Kurve, die zu keiner Lösung von $w^2 = x^4 + 2x^3 + 3x^2 + 2x$ führen, da $\xi = 1/x$ und $\eta = \frac{w}{x^2}$ mit $\xi, \eta, w \in \mathbb{Z}^+$ gelten soll. □

De Vogelaere fand allerdings noch viele weitere parametrische Lösungen von (4). In Zukunft lassen wir das t aus, da man es aus den anderen herleiten kann. Die einfachsten beiden Lösungen die De Vogelaere noch fand waren

$$z = [9, 3, 3], \quad x = [8, 1, 1], \quad y = [4, -1, 2] \tag{6}$$

und

$$z = [33, 3, 3], \quad x = [17, 11, -2], \quad y = [8, 17, 1]. \tag{7}$$

Eine der kompliziertesten Lösungen war

$$\begin{aligned} z &= [2577229375, -1371, 3525], \\ x &= [2232368805, 1861583, -2980], \\ y &= [968648234, 4964967, -1400]. \end{aligned} \tag{8}$$

Jede dieser Lösungen wird von einer weiteren Lösung begleitet, die zwar dieselben Werte für z und x hat, aber unterschiedliche y und t. So ist für (6) $y = [7, 5, 2]$ ebenfalls möglich und $y = [32, -1, -2]$ eine weitere Lösung mit den Werten von (7).

Nun stellt sich die Frage, ob man diesen Ansatz systematisieren kann und ob dies helfen kann die Gleichung (1) zu lösen. Der Weg dahin gliedert sich in 3 Schritte, welche wir im folgenden ausführen und erläutern werden.

1. Man zeige, dass es unendlich viele Lösungen in Parameterform von (4) gibt.

2. Man finde notwendige Bedingungen an die Koeffizienten der Lösungen in Parameterform sodass das biquadratische Polynom $t(u, v)$ möglicherweise einen quadratischen Wert annimmt.

[2]Nur ein Punkt auf E hat eine senkrecht zur y-Achse stehende Tangente - $2P$.

3. Zuletzt filtere man alle parametrischen Lösungen aus, die diese Bedingungen nicht erfüllen und teste die übrigen numerisch um zu sehen, ob sie eine Lösung von (1) bieten.

4 Der erste Schritt

Als erstes gilt es festzustellen, dass jeder der drei Ausdrücke x, y, z , welche durch homogene quadratische Polynome in zwei Variablen u und v gegeben sind, eine quadratische homogene Gleichung $Q(x, y, z) = 0$ erfüllen.

Beweis. In einem quadratischen homogenen Polynom dreier Variablen kann es zu den sechs Ausdrücken $x^2, y^2, z^2, xy, xz, yz$ kommen. Jedes dieser Ausdrücke ist als eine Linearkombination von u^4, u^3v, u^2v^2, uv^3 und v^4 ausdrückbar. Mithin muss es einen linearen Zusammenhang zwischen ihnen geben. Somit kann man sie als Lösung eines quadratischen homogenen Polynoms in drei Variablen schreiben. □

Es sei anzumerken dass die Umkehrung zwar über $\mathbb{C}$, aber nicht über $\mathbb{Q}$ stimmt. Ist Q ein homogenes quadratisches Polynom mit rationalen Koeffizienten, so kann man die Lösungen von $Q(x, y, z) = 0$ parametrisch genau dann durch drei binäre quadratische Formen mit rationalen Koeffizienten darstellen, wenn es mindestens eine rationale Lösung gibt.

Beweis. Diese Aussage beruht auf einem Prinzip Diophantus'. Eine quadratische Lösung mit rationalen Koeffizienten die eine rationale Lösung hat, hat unendlich viele. Sei P ein Punkt mit rationalen Koeffizienten auf der Lösungsmenge der quadratischen Gleichung. Jede Gerade durch P welche durch eine Gleichung mit rationalen Koeffizienten beschrieben wird schneidet unsere Lösungsmenge in einem weiteren Punkt mit rationalen Koordinaten. □

Somit entspricht jede der Escott-de-Vogelaere Lösungen von (4) einem quadratischen Zusammenhang. Für (5), (6), (7) und (8) sind dies folgende:

$$
\begin{aligned}
&x^2 + y^2 - xy + xz - yz = 0, \\
&5x^2 + 5y^2 + xy + 4z^2 - 7xz - 7yz = 0, \\
&13x^2 + 13y^2 - 17xy - 4z^2 + 7xz - 7yz = 0, \text{und} \\
&4261205(x^2 + y^2 - xy) - 1763124(xy + z^2) + 152303(yz - xz) = 0.
\end{aligned}
\tag{9}
$$

Da diese quadratischen Polynome (4) erfüllen, haben sie die Eigenschaft, dass

$$Q(x,y,z) = 0 \Rightarrow z^4 - x^4 - y^4 = \square \tag{10}$$

Wir teilen das Problem also in drei Teile

1. Wie lautet die generelle Form von Q, wenn (10) erfüllt ist?
2. Welche von diesen Polynomen haben eine rationale Lösung und führen somit zu einer parametrischen Lösung von (4)?
3. Welche dieser Lösungen könnten zu einem quadratischen t führen? Gibt es Bedingungen um die anderen Lösungen zu eliminieren?

Kümmern wir uns zuerst um die erste Frage.
Man schreibe F für den Ausdruck

$$F(x,y,z) = z^4 - x^4 - y^4. \tag{11}$$

Sodann sagt (10) aus, dass F ein Quadratrest modulo Q ist, also

$$F(x,y,z) = R(x,y,z)^2 - Q(x,y,z)S(x,y,z) \tag{12}$$

für geeignete Polynome $R(x,y,z)$ und $S(x,y,z)$. Betrachtet man den Grad der Polynome, so müssten diese ebenfalls quadratische Formen in x, y und z sein. Sehen wir uns noch einmal (5) an mit $Q = Q_0$ wie in (9), so erhalten wir

$$\begin{aligned} Q_0(x,y,z) &= x^2 + y^2 - xy + xz - yz, \\ R_0(x,y,z) &= z^2 - (x-y)^2, \\ S_0(x,y,z) &= 2(x^2 + y^2 - xy - xz + yz). \end{aligned} \tag{13}$$

Der Ausdruck $R^2 - QS$ entspricht (bis auf einen Faktor 1/4) der Diskriminante von $Q\xi^2 + 2R\xi\eta + S\eta^2$. Diese Diskriminante ist bekannterweise invariant bei Operation von $SL_2(\mathbb{Q})$, also unter linearen Transformationen der Form $(\xi\eta) \to (\xi\eta)M$, wobei $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Q})$ ist.[3]

[3] $SL_2(\mathbb{Q})$ ist die spezielle lineare Gruppe. Ihre Elemente sind jene 2×2 Matrizen mit rationalen Koeffizienten, für die die Determinante $\alpha\delta - \beta\gamma = 1$ ist.

Beweis. $(\xi\eta)M = (\xi\eta)\cdot\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = ((\xi\alpha+\eta\gamma)\ \ (\xi\beta+\eta\delta))$.
Aus $Q\xi^2+2R\xi\eta+S\eta^2$ wird also:

$$\begin{aligned}
&Q(\xi\alpha+\eta\gamma)^2+2R(\xi\alpha+\eta\gamma)(\xi\beta+\eta\delta)+S(\xi\beta+\eta\delta)^2\\
&=\xi^2(Q\alpha^2+2R\alpha\beta+S\beta^2)+2\xi\eta(Q\alpha\gamma+R\alpha\delta+R\beta\gamma+S\beta\delta)\\
&\quad+\eta^2(Q\gamma^2+2R\gamma\delta+S\delta^2)
\end{aligned}$$

Die Determinante Δ des Polynoms $Au^2+2Buv+Cv^2$ ist gegeben durch B^2-AC. Setzt man dies ein, so ist

$$\begin{aligned}
\Delta &= (Q\alpha\gamma+R(\alpha\delta+\beta\gamma)+S\beta\delta)^2\\
&\quad-\left(Q\alpha^2+2R\alpha\beta+S\beta^2\right)\left(Q\gamma^2+2R\gamma\delta+S\delta^2\right)\\
&= Q^2\alpha^2\gamma^2+R^2(\alpha\delta+\beta\gamma)^2+S^2\beta^2\delta^2+2Q\alpha\gamma R(\alpha\delta+\beta\gamma)\\
&\quad+2Q\alpha\gamma S\beta\gamma+2R(\alpha\delta+\beta\gamma)S\beta\delta\\
&\quad-(Q^2\alpha^2\gamma^2+Q\alpha^2 2R\gamma\delta+Q\alpha^2S\delta^2+2R\alpha\beta Q\gamma^2\\
&\quad+4R^2\alpha\beta\gamma\delta+2R\alpha\beta S\delta^2+S\beta^2Q\gamma^2+S\beta^2 2R\gamma\delta+S^2\beta^2+\delta^2)\\
&= R^2(\alpha^2\delta^2+\beta^2\gamma^2-2\alpha\beta\gamma\delta)\\
&\quad+QR(2\alpha\gamma(\alpha\delta+\beta\gamma)-2\alpha^2\gamma\delta-2\alpha\beta\gamma^2)+RS(2(\alpha\delta+\beta\gamma)\\
&\quad-2\alpha\beta\delta^2-2\beta^2\gamma\delta)+QS(2\alpha\gamma\beta\delta-\alpha^2\delta^2-\beta^2\gamma^2)\\
&= R^2(\alpha\delta-\beta\gamma)^2+QR(2\alpha\gamma(\alpha\delta+\beta\gamma-\alpha\delta-\beta\gamma))\\
&\quad RS(2\beta\delta(\alpha\delta+\beta\gamma-\alpha\delta-\beta\gamma))+QS(-(\alpha\delta-\beta\gamma)^2)
\end{aligned}$$

Da jedoch $M\in SL_2(\mathbb{Q})$, ist $\alpha\delta-\beta\gamma=1$. Somit ist die letzte Zeile äquivalent zu R^2-QS, der Determinante von $Q\xi^2+2R\xi\eta+S\eta^2$.
QED □

Wir können also unendlich viele Lösungen von (12) generieren, indem wir eine beliebige Matrix

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in SL_2(\mathbb{Q})$$

auf die besondere Lösung (13) anwenden. Wie bereits im vorangegangenen Beweis zur Invarianz der Determinante gezeigt, haben die Polynome Q,R und S dann die Form:

$$\begin{aligned}
Q(x,y,z) &= \alpha^2Q_0+2\alpha\beta R_0+\beta^2S_0,\\
R(x,y,z) &= \alpha\gamma Q_0+(\alpha\delta+\beta\gamma)R_0+\beta\delta S_0,\\
S(x,y,z) &= \gamma^2Q_0+2\gamma\delta R_0+\delta^2S_0. \qquad (14)
\end{aligned}$$

Zunächst konzentrieren wir uns allerdings nur auf Q.

Proposition 1. *Seien $A, B, C \in \mathbb{Q}$ gegeben durch*

$$A = \alpha^2 - 2\alpha\beta + 2\beta^2, \quad B = 2\alpha\beta, \text{sowie} \quad C = \alpha^2 - 2\beta^2 \tag{15}$$

für zwei rationale Zahlen α, β. Sodann erfüllt das Quadrik

$$Q_{A,B,C}(x, y, z) = A(x^2 - xy + y^2) + B(xy + z^2) + C(xz - yz) \tag{16}$$

die Eigenschaft (10).

Um dies zu beweisen genügt es, die Klammern auszumultiplizieren und die Terme zu ordnen. Durch erneutes einklammern zeigt sich, dass $Q_{A,B,C}$ wie erwünscht die Form $\alpha^2 Q_0 + 2\alpha\beta R_0 + \beta^2 S_0$ hat.

Wir stellen fest, dass

$$A^2 + 2AB - B^2 - C^2 = 0 \tag{17}$$

Andererseits werden alle Lösungen von (17) bis auf multiplikative konstanten von (15) generiert. Man kann also sagen, dass für jedes Tripel (A, B, C) welches (17) erfüllt das Quadrik (16) die Eigenschaft (10) hat. Wir wollen nun zeigen, dass wir auf diese Weise auch keine Lösungen verlieren. Der Autor des ursprünglichen Papers fasste diesen Beweis in sehr kurzer Form, weshalb wir ihn hier selbst weiter ausarbeiten.

Durch jede rationale Lösung soll zumindest eine der Quadriken $Q_{A,B,C}$ gehen.

Proposition 2. *Jede Lösung $(z, x, y, t) = (\zeta, \xi, \eta, \tau)$ von* (4) *erfüllt $Q_{A,B,C}(\xi, \eta, \zeta) = 0$ für* (17) *erfüllende rationale Zahlen A, B, C.*

Beweis. Setzt man $Q_{A,B,C} = 0$ und löst die Gleichung (16) nach C auf, so erhält man

$$C = \frac{A(\xi^2 - \xi\eta + \eta^2) + B(\xi\eta + \zeta^2)}{\zeta(\eta - \xi)}$$

Wir setzen dies nun in (17) ein:

$$\begin{aligned}
0 &= A^2 + 2AB - B^2 - \left(\frac{A(\xi^2 - \xi\eta + \eta^2) + B(\xi\eta + \zeta^2)}{\zeta(\eta - \xi)}\right)^2 \\
0 &= A^2(\zeta(\eta-\xi))^2 + 2AB(\zeta(\eta-\xi))^2 - \\
&\quad B^2(\zeta(\eta-\xi))^2 - (A(\xi^2 - \xi\eta + \eta^2) + B(\xi\eta + \zeta^2))^2 \\
0 &= \left(\frac{A}{B}\right)^2 (\zeta^2(\eta-\xi)^2 - (\xi^2 - \xi\eta + \eta^2)^2) \\
&\quad +2\frac{A}{B}(\zeta^2(\eta-\xi)^2 - (\xi^2 - \xi\eta + \eta^2)(\xi\eta + \zeta^2)) \\
&\quad +((\xi\eta + \zeta^2)^2 - \zeta^2(\eta-\xi)^2)
\end{aligned}$$

Dies ist eine quadratische Gleichung für das Verhältnis $A : B$. Da $A, B \in \mathbb{Q} \setminus 0$ soll auch $\frac{A}{B} \in \mathbb{Q}$ sein. Eine rationale Lösung hat eine quadratische Gleichung allerdings nur, wenn ihre Diskriminante ein Quadrat ist. In diesem Falle ist die Diskriminante

$$\begin{aligned}
\Delta &= (\zeta^2(\eta-\xi)^2 - (\xi^2 - \xi\eta + \eta^2)(\xi\eta + \zeta^2))^2 \\
&\quad -4 \cdot \left((\zeta^2(\eta-\xi)^2 - (\xi^2 - \xi\eta + \eta^2)^2) \cdot ((\xi\eta + \zeta^2)^2 - \zeta^2(\eta-\xi)^2)\right)
\end{aligned}$$

Die Diskriminante ist das Produkt aus dem Quadrat einer Funktion in ξ, η, ζ sowie der Fermat-Kurve $F = \zeta^4 - \eta^4 - \xi^4$, von der wir ausgehen dass sie einem Quadrat entspricht. Somit hat die Gleichung für $A : B$ eine Lösung und mithilfe der Mitternachtsformel ist diese berechenbar. Setzt man dann noch C wie oben ein, so erhält man die Gleichungen

$$\begin{aligned}
A &= (\xi^2 + \zeta^2)(\eta^2 + \zeta^2) \\
B &= -\xi\eta(\xi^2 + \eta^2 + \zeta^2 - \xi\eta) - \tau\zeta(\xi - \eta), \\
C &= -\zeta(\xi - \eta)(\xi^2 + \eta^2 + \zeta^2) + \tau(\xi\eta + \zeta^2)
\end{aligned} \tag{18}$$

Diese A, B, C erfüllen (17) und $Q_{A,B,C} = 0$. QED □

5 Existenz eines Rationalen Punktes auf $Q = 0$

Wir untersuchen nun, wann eine der in (16) gegebenen Kurven eine rationale Nullstelle hat. A, B und C sind durch (15) gegeben, da alle (17) erfüllende Tripel so aussehen, unter Missachtung einer mutliplikativen Konstante.

Proposition 3. *Seien $\alpha, \beta \in \mathbb{Q}$ und $Q = Q_{A,B,C}$ die in Proposition 1 definierte quadratische Form. Dann hat $Q(x, y, z) = 0$ genau dann eine nichttriviale Lösung wenn sowohl $A+B = \alpha^2+2\beta^2$ als auch $A-B = \alpha^2-4\alpha\beta+2\beta^2$ die Summe aus zwei Quadraten rationaler Zahlen sind.*

Beweis. Das Lokal-Global-Prinzip von Hasse und Minkowski besagt, dass eine Gleichung über den rationalen Zahlen genau dann gelöst werden kann, wenn sie über die reellen Zahlen und den p-adischen Zahlen gelöst werden kann. Speziell hat also die quadratische Form $Q = 0$ nur dann eine Lösung über $\mathbb{Q}$. wenn sie eine reelle und eine Lösung modulo $p^n \forall n$ hat, und dies für jede Primzahl p. Hilbert bewies, dass es ausreichend ist die p-adischen Lösungen für ungerade p zu überprüfen. Man wähle α und β ganzzahlig und teilerfremd[4]. Die Diskriminante von Q ist dann, bis auf ein Vorzeichen und einer Zweierpotenz, gleich $AB(A-B)(A+B)$. Ist p eine ungerade Primzahl, die AB teilt, so gibt es dafür nur 3 Fälle. $AB = (\alpha^2 - 2\alpha\beta + 2\beta^2)2\alpha\beta$. Da p das Produkt teilt, teilt es mindestens einen der Faktoren (Euklids Lemma). p ist ungerade, also kann man die 2 ignorieren. Dann ist also entweder $\alpha \equiv 0 \pmod{p}$ oder $\beta \equiv 0 \pmod{p}$ oder aber $\alpha^2-2\alpha\beta+2\beta^2 \equiv 0 \pmod{p}$. Letzteres ist äquivalent zu $(\alpha-\beta)^2 \equiv -\beta^2 \pmod{p} \Leftrightarrow \alpha-\beta \equiv i\beta, \quad i^2 \equiv -1 \pmod{p}$. Dann ist $\alpha \equiv (1+i)\beta \pmod{p}$. Sodann hat $Q = 0$ p-adische Lösungen.

Sollte p die Zahl $A + B = \alpha^2 + 2\beta^2$ in ungerader Potenz teilen, so ist $Q \equiv \square - 2\square$,[5] weshalb $Q = 0$ genau dann eine Lösung im Körper $\mathbb{Q}_p$ der p-adischen Zahlen hat wenn 2 eine Quadratwurzel in dem Körper hat, also eine Zahl die $i^2 \equiv 2 \pmod{p}$ erfüllt. Dafür muss $p \equiv \pm 1 \pmod{8}$ sein, wie das quadratische Reziprozitätsgesetz besagt.

Wir wollen hierfür einen Beweis ansprechen, der das Legendre-Symbol benutzt. Für ungerade p gibt $\left(\frac{a}{p}\right)$ an, ob a ein quadratischer Rest modulo p ist. Es gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Dies ist 0, wenn a durch p teilbar ist, 1 wenn es ein quadratischer Rest ist und -1 wenn nicht. Man betrachte Menge $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ modulo p. Von all den Resten zählt man nun die, die $> p/2$ sind und nenne diese Anzahl N. Gauß's Lemma besagt nun, dass $\left(\frac{a}{p}\right) = (-1)^N$, wenn $ggT(a, p) = 1$. In unserem Falle also suchen wir

[4]Existieren rationale α und β, für die Q eine Lösung hat, so kann man diese in teilerfremde ganze Zahlen verwandeln ohne die Lösung zu verändern.

[5]Denn die Diskriminante muss p in gerader Potenz enthalten, weshalb $p^{ungerade} \mid AB(A-B)$ und daher, da AB in gerader Potenz geteilt wird, $A - B = \square - 2\square \equiv 0 \pmod{p}$, wobei keine der beiden Zahlen $\square$ und $2\square$ von p geteilt wird.

die Anzahl Reste von $\{2, 4, \ldots, p-1\}$ modulo p, die größer als $p/2$ sind. Ist $p \equiv 1 \pmod 8$, dann kann man es schreiben als $8k+1$, weshalb die Menge $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ genau $4k$ Elemente enthält. Unsere Zusatzbedingung schließt all jene geraden Zahlen, also Zahlen der Form $2i$, aus, die $\leq p/2$ sind. Somit wäre $i \leq p/4 \Leftrightarrow i \leq 2k + \frac{1}{4}$. Dies sind $2k$ Zahlen, und somit ist $N = 4k - 2k$ also eine gerade Zahl, weshalb $\left(\frac{2}{p}\right) = 1$ ist. Analog ist für $p = 8k+7$ $N = 2k+2$ während bei $p = 8k \pm 3$ N jeweils $2k+1$ und somit ungerade ist. Also muss nun $p \equiv \pm 1 \pmod 8$ sein. Da aber $p \mid (\alpha^2 + 2\beta^2)$ gilt, muss $p \equiv 1$ oder $3 \pmod 8$ bekannterweise gelten. Somit ist $p \equiv 1 \pmod 8 \Rightarrow p \equiv 1 \pmod 4$.

Also wissen wir, dass $\alpha^2 + 2\beta^2$ ein Quadrat oder das Doppelte eines Quadrates ist, multipliziert mit dem Produkt von Primzahlen $\equiv 1 \pmod 4$. Der Zwei Quadrate Satz sagt nun, dass eine Zahl n genau dann als Summe zweier Quadratzahlen schreibbar ist, wenn ihre Primfaktoren $\equiv 3 \pmod 4$ in gerader Potenz auftauchen. In unserem Falle gibt es keine solchen, also muss $\alpha^2 + 2\beta^2$ Summe zweier Quadratzahlen sein.

Auf ähnliche Weise kann man nun argumentieren, dass wenn eine Primzahl p in ungerader Potenz $(A - B) = (\alpha - 2\beta)^2 - 2\beta^2$ teilt, dann muss $Q = \square + 2\square$ sein. Dann ist $Q = 0$ in $\mathbb{Q}_p$ äquivalent zu der Aussage, dass $p \equiv 1$ oder $3 \pmod 8$ ist. Und da $p \equiv \pm 1 \pmod 8$ sowieso gelten muss, ist $p \equiv 1 \pmod 4$. Da zudem $\alpha^2 - 4\alpha\beta + 2\beta^2$ positiv sein muss, kann man es als Produkt von Primzahlen $\equiv 1 \pmod 4$ mal einen Quadrat oder dem Doppelten eines Quadrates schreiben. Damit ist auch $A - B$ die Summe zweier Quadrate. □

Beweis des Gauß Lemmas. Im vorangegangenen Beweis benutzten wir das Gauß Lemma. Dieses wollen wir auch gleich beweisen. Und zwar zählen wir das Produkt der Zahlen $a, 2a, \ldots, \frac{p-1}{2}a$ auf zwei Weisen modulo p. Zum einen ist dieses Produkt gleich $a^{\frac{p-1}{2}} \cdot \frac{p-1}{2}!$. Andererseits kann man jeden Rest $i \pmod p$ auch schreiben als $-(p-i) \pmod p$, weshalb alle jene Reste, die größer als $p/2$ modulo p sind, durch ihre Komplementärreste mal (-1) ausgedrückt werden können. Es gibt zudem keine zwei Komplementärreste modulo p in $a, 2a, \ldots, \frac{p-1}{2}a$, da ansonsten $k_1 a \equiv -k_2 a$ gälte. Da nun aber a teilerfremd zu p ist, ist dies äquivalent zu der Aussage, dass $k_1 \equiv -k_2 \pmod p$ ist. Doch sind alle Vorfaktoren $\leq \frac{p-1}{2}$, weshalb dies nicht möglich ist.

Es bezeichnet N die Anzahl der Zahlen, deren Vorzeichen wir umdrehen um $< p/2 \pmod p$ zu werden. Somit ist $a \cdot 2a \cdot \cdots \cdot \frac{p-1}{2}a \equiv (-1)^N \cdot (1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2})$

	α	β	A	B	C	ξ	η	ζ
	1	−6	85	−12	−71	6	3	7
	1	−2	13	−4	−7	2	2	3
∗	1	0	1	0	1	0	0	−1
	1	2	5	4	−7	1	−2	−3
	1	6	61	12	−71	27	8	53
	3	−8	185	−48	−119	25	14	27
	3	−4	65	−24	−23	1	2	3
	3	−2	29	−12	1	−3	2	7
	3	8	89	48	−119	4	−3	13
∗	5	−8	233	−80	−103	20	5	21
	7	−6	205	−84	−23	31	20	33
∗	7	−4	137	−56	17	38	2	63
	9	−4	185	−72	49	−3	4	13
	9	2	53	36	73	2	−3	−7
	11	−6	325	−132	49	7	8	9

Tabelle 1: Die ersten Quadriken mit einer rationalen Nullstelle (ξ, η, ζ)

Also ist $a^{\frac{p-1}{2}} \cdot \frac{p-1}{2}! \equiv (-1)^N \cdot \frac{p-1}{2}! \pmod{p}$. Die Fakultät ist zudem teilerfremd zu p und somit ist $a^{\frac{p-1}{2}} \equiv (-1)^N \pmod{p}$, also $\left(\frac{a}{p}\right) = (-1)^N$ per Definition des Legendre-Symbols.

□

Ab jetzt werden wir numerisch nach weiteren Lösungen suchen. Hierfür eigneten wir uns die Programmiersprache GAP an. Und zwar suchen wir all jene α und β, die Proposition 3 erfüllen. Der Einfachheit halber kann man annehmen, dass $\alpha, \beta \in \mathbb{Z}$ gilt. Außerdem suchen wir nun begrenzte α und β, also solche, sodass $\alpha^2 + 2\beta^2 \leq 200$. Außerdem können wir α und β durch ihren ggT teilen, ohne Lösungen zu verlieren, also können wir (zum Sparen von Rechenarbeit) annehmen, dass $ggT(\alpha, \beta) = 1$ und somit α ungerade und β gerade ist. Andernfalls kann man α, β ersetzen durch $\beta, \frac{1}{2}\alpha$. Dann wird A, B, C zu $\frac{1}{2}A, \frac{1}{2}B$ und $-\frac{1}{2}C$, was aufgrund der in A und B vorliegenden Symmetrie von x, y keine wesentlichen neuen Lösungen zur Folge hat. In der Tabelle stehen ebenfalls A, B, C sowie die Lösungen (ξ, η, ζ), welche von uns mithilfe eines Programmes gesucht wurden.

Proposition 4. *Es gibt unendlich viele $\alpha : \beta \in \mathbb{Q}$ sodass das in Proposition*

1 *definierte Quadrik einen rationalen Punkt hat.*

Beweis. Man nutze den Beweis von Proposition 2. Man nehme (5) als eine Lösung von (4). Diese parametrische Lösung hat unendlich viele rationale Lösungen (ξ, η, ζ, τ). Für diese geben (19) jeweils zwei Quadriken in der Form (16), welche durch (ξ, η, ζ) gehen. Da wir nämlich τ also Wurzel von $F(\xi, \eta, \zeta)$ nehmen, haben wir zwei mögliche Werte: τ und $-\tau$. Eine dieser beiden Quadriken entspricht der, mit der wir starteten, nämlich Escott's Lösung. die andere jedoch ist verschieden von der ersten. Somit kriegt man unendlich viele Quadriken der erwünschten Form, welche mindestens einen rationalen Punkt enthalten. □

Setzt man zum Beispiel die Escott-Lösung, also $\xi = [0, 1, 0], \quad \eta = [0, 1, 1], \zeta = [1, 1, 1]$ ein mit $t = -[1, 2, 3, 2, 0]$, da wir ja diesmal den negativen Term benutzen. Dann wird aus A, B und C, wie im Beweis Proposition 2 durch die Variablen ausgedrückt,

$$\begin{aligned}
A &= [0,0,0,0,1,2,1,0,0] + [0,0,1,2,3,2,1,0,0] + [0,0,1,4,8,10,8,4,1] \\
&\quad +[1,4,10,16,19,16,10,4,1] \\
&= [1,4,12,22,31,30,20,8,2] \\
B &= [0,0,0,0,1,2,1,0,0] + [0,1,3,6,7,5,2,0,0] - [0,0,0,0,1,1,0,0,0] \\
&\quad -[0,0,1,3,5,5,3,1,0] - [0,0,0,0,1,3,3,1,0] - [0,1,4,9,13,12,7,2,0] \\
&= [0,0,-2,-6,-12,-14,-10,-4,0] \\
C &= [0,0,0,1,2,2,1,0,0] + [0,0,0,1,4,7,7,4,1] + [0,1,4,9,13,13,9,4,1] \\
&\quad -[0,0,0,1,3,4,3,1,0] - [0,1,3,6,7,6,3,1,0] - [0,0,0,1,1,1,0,0,0] \\
&\quad -[0,0,1,3,5,5,2,0] - [1,4,10,16,18,14,7,2,0] \\
&= [-1,-4,-10,-16,-15,-8,2,4,2]
\end{aligned}$$

6 Herausfiltern unproduktiver Lösungen

Nun analysieren wir die Lösungen, die wir mithilfe von Proposition 8 kriegen können. Man nehme an, man hat eine Lösung gefunden, sodass $Q(\xi, \eta, \zeta) = 0$. Dies kann einfach per Ausprobieren machen, in Tabelle 1 finden sich einige

Lösungen. Die parametrische Lösung wird dann gegeben durch

$$\begin{aligned} x &= [A\xi, C(\eta-\xi) - 2B\zeta, (B-A)\eta], \\ y &= [A\eta, -C(\eta-\xi) + 2B\zeta, (B-A)\xi], \\ z &= [A\zeta, (B-3A)(\eta-\xi) + 2C\zeta, (A-B)\zeta]. \end{aligned} \tag{19}$$

Hierfür macht man die Werte von $u = 0$ und von $v = 0$ proportional zu den bekannten Lösungen (ξ, η, ζ) und $(\eta, \xi, -\zeta)$. Anschließend löst man nach dem mittleren Koeffizienten aus.

Abziehen der drei Gleichungen in vierter Potenz voneinander liefert einem ein Polynom für t^2, welches man dann überprüfen kann. Anzumerken ist hier, dass das von Ph.D. Don Zagier gegebene Polynom für t im Spezialfall zwar korrekt ist, im allgemeinen jedoch nicht. Das Polynom $t = t(u, v)$

$$t = [A^2\lambda, A\mu, (A-B)\mu, (A-B)^2\lambda], \tag{20}$$

mit

$$\begin{aligned} \lambda &= -\left(\zeta^2 - (\xi-\eta)^2 + \frac{2B}{A+B-C}(\xi^2 - \xi\eta + \eta^2 + \xi\zeta - \eta\zeta)\right) \\ &= -\left(\frac{A-B}{C}(\xi^2 - \xi\eta + \eta^2) - \frac{A+B}{C}(\xi\eta + \zeta^2)\right), \\ \mu &= -\left(2(B+A)(\xi^2 + \xi\eta + \eta^2) + 2(B-2A)\zeta^2\right), \\ v &= -(C(A-B)(\xi^2 + \eta^2) + 2C(A+B)\xi\eta + 2C(2B-3A)\zeta^2 \\ &\quad -4(2A^2 - 2AB + B^2)\zeta(\xi-\eta)). \end{aligned} \tag{21}$$

nämlich ist im allgemeinen nicht die Wurzel aus dem Polynom, welches man bei Abzug der Gleichungen erhält.

Wir wollen die Verhältnisse $\alpha : \beta$ kennen, bei denen t selbst ein Quadrat sein kann. Analog zu Proposition 3 existiert dafür ein Kriterium:

Proposition 5. *Damit die Lösungsfamilie von (α, β) ein Element $t = \pm\square$ enthält, dürfen $A = \alpha^2 - 2\alpha\beta + 2\beta^2$ sowie $A + 2B = \alpha^2 + 2\alpha\beta + 2\beta^2$ (ebenso wie $A + B$ und $A - B$) keine Primzahl $\not\equiv 1 \pmod 8$ in ungerader Potenz enthalten.*

Beweis. Der Beweis läuft ähnlich wie der letzte. Ist p eine ungerade Primzahl, die $\alpha^2 - 2\alpha\beta + 2\beta^2$ in ungerader Potenz teilt, dann ist $\alpha/\beta = 1 + i$ mit $i^2 \equiv -1$

(mod p). Also muss $p \equiv 1 \pmod 4$ sein. Dann sind Q und R wie in (14) durch

$$Q \equiv (2+2i)(\xi^2 - \xi\eta + \eta^2) + (2i-2)(\xi\zeta - \eta\zeta),$$
$$R \equiv i(\xi^2 - \xi\eta + \eta^2) + (\zeta^2 + \xi\eta) + (1+i)(\xi\zeta - \eta\zeta),$$

gegeben und daher

$$Q - 2R \equiv -2i(\xi - \eta - i\zeta)^2.$$

Eine Lösung von $Q = 0$, $R = \square$ ist also nur möglich wenn i ein Quadrat modulo p ist. Dafür muss jedoch $p \equiv 1 \pmod 8$ sein. Denn dann existiert ein k mit $k^2 \equiv i \pmod p$, $k^4 \equiv -1 \pmod p$ und $k^8 \equiv 1 \pmod p$. Somit muss $ord_p(k) = 8$ sein, da diese Ordnung 8 teilt aber weder 2 noch 4 entsprechen kann. Da aufgrund des kleinen Satzes von Fermat aber $k^{p-1} \equiv 1 \pmod p$ und die Ordnung einer Zahl jede Zahl v teilt mit $k^v \equiv 1 \pmod p$, teilt 8 die Zahl $p - 1 \Rightarrow p \equiv 1 \pmod 8$.

Ähnlich kann man für $p \mid \alpha^2 + 2\alpha\beta + 2\beta^2$ argumentieren. $\square$

7 Die Suche nach Lösungen von $z^4 = w^4 + x^4 + y^4$

Wir kommen nun zum letzten Schritt: mithilfe unserer bisherigen Ergebnisse suchen wir nach Lösungen der Gleichung (1). Die mit einem Sternchen markierten Zeilen in der Tabelle 1 sind jene α, β welche die Zusatzbedingungen erfüllen. Die erste Zeile führt zu Escotts Lösung, von der wir wissen, dass sie keine Lösungen für uns enthält. Setzt man nun all die Werte ein, die wir haben, so erhält man (x_1, y_1, z_1) und (x_2, y_2, z_2) mit

$$x_1 = [20 \cdot 233, 4905, -5 \cdot 313], \quad x_2 = [38 \cdot 137, 6444, -2 \cdot 193],$$
$$y_1 = [5 \cdot 233, -4905, -20 \cdot 313], \quad y_2 = [2 \cdot 137, -6444, -38 \cdot 193],$$
$$z_1 = [21 \cdot 233, 7359, 21 \cdot 313], \quad z_2 = [63 \cdot 137, 18954, 63 \cdot 193].$$

Die dazugehörigen t-Polynome sind:

$$t_1(u,v) = [184 \cdot 233^2, 320922 \cdot 233, 130661741, 320922 \cdot 313, 184 \cdot 313^2]$$
$$t_2(u,v) = [3697 \cdot 137^2, 2372652 \cdot 137, 573811862, 2372652 \cdot 193, 3697 \cdot 193^2]$$

Eine Computersuche gibt als erste Lösung $t_1(61, 5) = 15365639^2$,

$$20615673^4 = 18796760^4 + 2682440^4 + 15365639^4.$$

Diese Lösung generiert unendlich viele weitere Lösungen. Denn die eliptische Kurve $Y^2 = t_1(X, 1)$ hat den Punkt $(61/5, 15365639/25)$ hat unendliche Ordnung und gibt somit unendlich viele weitere Lösungen durch Punktverdopplung.

Die Gleichungen $t_2(u, v) = \pm w^2$ haben keine Lösungen mit $0 < \max(|\ u\ |, |\ v\ |) \leq 500$. Man kann die Tabelle erweitern durch größere Suchen und dank der Kriterien also mit Computerhilfe weitere Lösungen bestimmen.

8 Erstes Fazit

Auf beliebige Potenzen lassen sich die angewandten Methoden nicht verallgemeinern. Dies rührt daher, dass speziell Biquadratische Kurven zur Lösung intensiv benutzt wurden. An einigen wichtigen Stellen wurden Eigenschaften dieser Kurven und von Quadriken benutzt. Somit braucht man für andere Potenzen andere Ideen.

Jedoch kann man die Methoden versuchen anzuwenden, um Exponenten zu betrachten, welche durch 4 teilbar sind. Jene sind auch biquadratisch. Speziell wollen wir uns daher auf Exponenten der Form 2^k konzentrieren und dort versuchen Ergebnisse zu erzielen. Wir werden dafür anfangen mit 8-ten Potenzen und Lösungen der Gleichung $z^8 = x^8 + y^8 + w^8$ suchen.

Von da aus kann man sich an Verallgemeinerungen herantasten.

9 Ersetzen einer vierten durch eine achte Potenz

Um die Gleichung

$$z^8 = x^8 + y^8 + w^8 \tag{22}$$

zu lösen, versuchen wir erst einmal auf Basis der Lösungen für (1) die Gleichung

$$z^4 = x^4 + y^4 + w^8 \tag{23}$$

zu lösen.

Dafür wollen wir dieselben Ideen anwenden, die Zagier anwandte, um aus den Lösungen von (4) Lösungen von (1) zu generieren.

Ebenso kann es nützlich sein, die Polynome für x, y, z auf quadratische Eigenschaften zu untersuchen, dies auch wieder entweder mit Computersuche

oder aber indem wir den gesamten Lösungsweg Zagiers noch einmal durchgehen mit einem Variablenwechsel.

Proposition 6. *Damit t eine vierte Potenz sein kann, w also eine achte, darf keine Primzahl $\not\equiv 1 \pmod{16}$ die Zahlen A und $A + 2B$ in ungerader Potenz teilen.*

Beweis. Wir betrachten erneut $Q - 2R \equiv -2i(\xi - \eta - i\zeta)^2 \pmod{p}$. Nun kann man Lösungen (ξ, η, ζ) mit beliebigen ganzen oder rationalen Zahlen multiplizieren und es sind weiterhin Lösungen, welche man auch für Q und R verwenden könnte. Nun sei $\xi' = \xi \cdot (\xi - \eta - i\zeta)^2$, $\eta' = \eta \cdot (\xi - \eta - i\zeta)^2$ und $\zeta' = \zeta \cdot (\xi - \eta - i\zeta)^2$. Sodann ist $Q - 2R \equiv -2i(\xi' - \eta' - i\zeta')^2 = -2i(\xi - \eta - i\zeta)^4$, weshalb also, damit R ein biquadratischer Rest sein kann, i ein biquadratischer Rest modulo p sein. Somit existiert ein k mit $k^8 \equiv -1 \pmod{p}$, also $k^{16} \equiv 1 \pmod{1}6$. Da nun die Ordnung $ord_p(k)$ 16 teilen muss aber weder 1, 2, 4 noch 8 sein kann (sonst wäre $k^8 \equiv 1 \pmod{16}$), muss die Ordnung selbst ebenfalls 16 sein und damit die Primzahl selbst $\equiv 1 \pmod{16}$, da $k^{p-1} \equiv 1 \pmod{16}$ (kleiner Satz von Fermat) und die Ordnung, also 16, diese Zahl teilen muss. Ähnliches lässt sich erneut mit $p \mid A + 2B$ machen. □

Verallgemeinert man diesen Beweis so kann man einfach zeigen, dass t nur dann eine 2^k-te Potenz sein kann, wenn keine Primzahl $\not\equiv 1 \pmod{2^{k+1}}$ A oder $A + 2B$ teilt.

Somit ist es wahrscheinlich, dass $f(n)$ nicht streng monoton wächst, denn obwohl solche Quadriken immer seltener werden für wachsende 2^k, so gibt es sie doch. Können wir das Verfahren auf die anderen Variablen erweitern, so ist es unwahrscheinlich keine Lösungen für eine gegebene Zweierpotenz zu finden.

10 Anhang

In diesem Anhang fügen wir einige Bilder von den Programmen und deren Ergebnisse ein. Die Abbildungen 5 bis 8 zeigen das Programm, welches wir letztlich aufstellten um im allgemeinen Lösungen der Gleichung $z^4 = x^4 + y^4 + w^4$ zu finden. Das Programm brachte uns bisher folgende zwei, noch nicht von Zagier gefundene Lösungen:

$$164925384^4 = 150374080^4 + 21459520^4 + 122925112^4$$

$$3858636950025^4 = 145549535000^4 + 383895784000^4 + 3524413775^4$$

```
gap> Quadrics := function( a , b )
> while a * a + 2 * b * b <= 200 do
>  if Gcd(a,b)=1 then
>  if TwoSquares(a * a + 2 * b * b) <> fail then
>  if a * a - 4 * a * b + 2 * b * b > 0 then
>  if TwoSquares(a * a - 4 * a * b + 2 * b * b) <> fail then
>       d:= a * a - 2 * a * b + 2 * b * b;;
>       e:= 2 * a * b;;
>       f:= a * a - 2 * b * b;;
>       Print("a=",a,",","b=",b,",","A=",d,",","B=",e,",","C=",f,"\n");
>  fi;
>  fi;
>  fi;
>  fi;
>  if a * a + 2 * (b + 2) * (b + 2) <= 200 then
>       b := b + 2;
>  else
>       a := a + 2;;
>       c := a;;
>       b := -10;;
>       if a * a + 2 * b * b > 200 then
>                while a * a + 2 * b * b > 200 do
>                       if 2 * b * b <=200 then
>                              b:= b+2;
>                       else
>                              a:=0;;
>                              b:=0;;
>                       fi;
>                od;
>       fi;
>       a := c;
>  fi;
> od;
> end;
function( a, b ) ... end
gap> Quadrics(1,-8);
a=1,b=-6,A=85,B=-12,C=-71
a=1,b=-2,A=13,B=-4,C=-7
a=1,b=0,A=1,B=0,C=1
a=1,b=2,A=5,B=4,C=-7
a=1,b=6,A=61,B=12,C=-71
a=3,b=-8,A=185,B=-48,C=-119
a=3,b=-4,A=65,B=-24,C=-23
a=3,b=-2,A=29,B=-12,C=1
a=3,b=8,A=89,B=48,C=-119
a=5,b=-8,A=233,B=-80,C=-103
a=7,b=-6,A=205,B=-84,C=-23
a=7,b=-4,A=137,B=-56,C=17
a=9,b=-4,A=185,B=-72,C=49
a=9,b=2,A=53,B=36,C=73
a=11,b=-6,A=325,B=-132,C=49
gap>
```

Abbildung 2: Programm für $\alpha^2 + 2\beta^2 \leq 200$

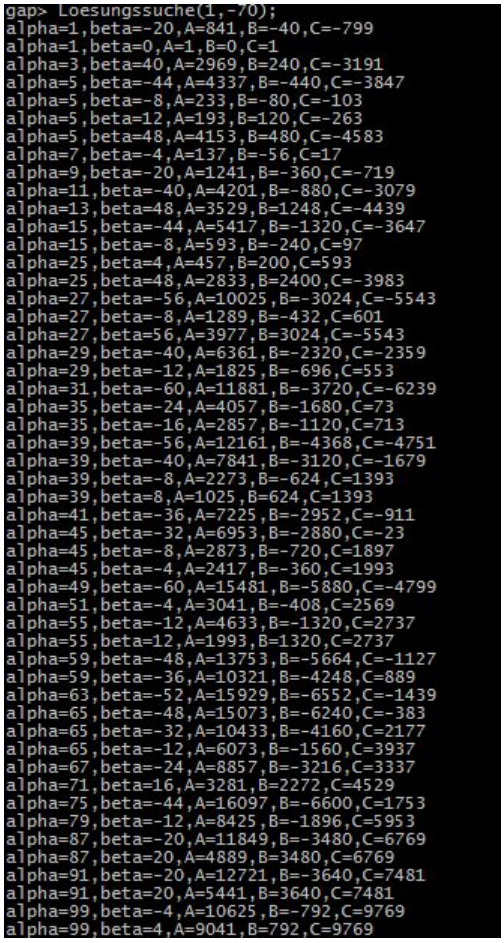

Abbildung 3: Mögliche Quadriken zur Lösung von 1 mit $\alpha^2 + 2\beta^2 \leq 10000$

Kleine Modifikationen liefern ein Programm, welches die Gleichung 23 lösen kann anhand unserer Kriterien. Abbildung 9 zeigt, welche Quadriken zur Lösung in Frage kommen. Jedoch konnten wir mit unserem Computer nicht mehr nachrechnen, wann und ob diese Quadriken tatsächlich Lösungen haben, da die benötigte Rechenzeit sehr hoch ist.

```
u:=0;;
v:=0;;
t:=0;;
A:=0;;
B:=0;;
C:=0;;
D:=0;;
F:=0;;
o:=0;;
l:= 1482940527301927;;

RootIntCeiling := function(n)
  if n = 0 then
    return 0;
  fi;
  return 1 + RootInt(n-1);
end;

tTest := function(n);
    if RootInt(n) = RootIntCeiling(n) then
        return true;
    else
        return false;
    fi;
end;

tSuche := function(u,v)
    A:= 184 * 233 * 233;;
    B:=320922 * 233;;
    C:=130661741;;
    D:=320922 * 313;;
    F:=184 * 313 * 313;;
    for u in [1..100] do
        for v in [1..100] do
            t:=A * (u ^ 4) + B * ( u ^ 3) * v + C * u * u * v * v + D * u * (  v ^ 3) + F * (v ^ 4);;
            o:= RootInt(t);
            if tTest(t) = true then
                Print("u=",u,",v=",v,",t=",t,",w=",o,"\n");
            fi;
        od;
    od;
end;
```

```
gap> tSuche(0,0);
u=61,v=5,t=236102861878321,w=15365639
gap>
```

Abbildung 4: Programm zum Suchen von Lösungen für ein spezifisches t-Polynom

```
tSuche := function(a,b,d,e,f,xi,eta,zeta)


    SuchStop:=0;;
    for u in [1..5000] do
        if SuchStop=0 then
        for v in [1..5000] do
            if SuchStop=0 then
            my:=(d * zeta * u^2 + ((e-3*d) * (eta - xi)+2 * f * zeta) * u * v + (d-e) * zeta * v^2)^4;;
            nu:=(d * xi * u^2 + (f * (eta-xi)-2 * e * zeta) * u * v+(e-d) * eta * v^2)^4;;
            lambda:=(d * eta * u^2 + (-f * (eta-xi)+2 * e * zeta) * u * v + (e-d) * xi * v^2)^4;;
            te:=my-lambda-nu;;
            if te>0 then
            if tTest(te)=true then
                t:=RootInt(te);
            if t>0 then
                o:= RootInt(t);
                if a<>1 then
                    if tTest(t) = true then
                        Print("alpha=",a,",beta=",b,",A=",d,",B=",e,",C=",f,",u=",u,",v=",v,",t=",t,",w=",o,"\n");
                        SuchStop:=1;;
                    fi;
                else
                    if b<>0 then
                        if tTest(t) = true then
                            Print("alpha=",a,",beta=",b,",A=",d,",B=",e,",C=",f,",u=",u,",v=",v,",t=",t,",w=",o,"\n");
                            SuchStop:=1;;
                        fi;
                    fi;
                fi;
            fi;
            else
                continue;
            fi;
            fi;
            fi;
        od;
        else
            continue;
        fi;
    od;
    if SuchStop=0 then
    Print("Nichts gefunden","\n");
    fi;
end;
```

Abbildung 5: Programm um allgemeine Lösungen der Gleichung $z^4 = x^4 + y^4 + w^4$ zu finden

```
SearchSol := function( d , e , f )
s:=0;;
i:=1;;
Stop:=0;;
while s < 1 do
    for z in [-175..175] do
    if s < 1 then
        for y in [-175..175] do
            if s < 1 then
            for x in [-175..175] do
                if i = 80000 then
                    i:=1;;
                    Print("calculating...");
                else
                    continue;
                fi;
                if s < 1 then
                Q:= d * ( x * x - x * y + y * y) + e * ( x * y + z * z) + f * ( x * z - y * z );;
                if Q = 0 then
                    if x = 0 then
                        if y = 0 then
                            if z = 0 then
                                continue;
                            else
                                s := s + 1;;
                                xi:=x;;
                                eta:=y;;
                                zeta:=z;;
                            fi;
                        else
                            s := s + 1;;
                            xi:=x;;
                            eta:=y;;
                            zeta:=z;;
                        fi;
                    else
                        s := s + 1;;
                        xi:=x;;
                        eta:=y;;
                        zeta:=z;;
                    fi;
                fi;
            fi;
            od;
        fi;
        od;
    i:=i+1;;
    fi;
```

Abbildung 6:

```
Loesungssuche := function( a , b )
while a * a + 2 * b * b <= 2000 do
 if Gcd(a,b)=1 then
 if TwoSquares(a * a + 2 * b * b) <> fail then
 if a * a - 4 * a * b + 2 * b * b > 0 then
 if TwoSquares(a * a - 4 * a * b + 2 * b * b) <> fail then
    d:= a * a - 2 * a * b + 2 * b * b;;
    e:= 2 * a * b;;
    f:= a * a - 2 * b * b;;
    Zaehler:=0;;
        HilfA:=d;;
        for p in PrimeDivisors(d) do
            if RemInt(p,8)<>1 then
                if Zaehler<>1 then
                    while Zaehler=0 do
                        if GcdInt(HilfA,p^2)=p^2 then
                            HilfA:=HilfA / (p^2);;
                        elif GcdInt(HilfA,p^2)=p then
                            Zaehler:=1;;
                        else
                            Zaehler:=2;;
                        fi;
                    od;
                else
                    continue;
                fi;
                if Zaehler=2 then
                    Zaehler:=0;;
                fi;
            fi;
        od;

        if Zaehler<>1 then
            HilfAB:=d+2*e;;
            for p in PrimeDivisors((d + 2 * e)) do
                if  RemInt(p,8)<>1 then
                    if Zaehler<>1 then
                        while Zaehler=0 do
                            if GcdInt(HilfAB,p^2)=p^2 then
                                HilfAB:=(HilfAB / (p^2));;
                            elif GcdInt(HilfAB,p^2)=p then
                                Zaehler:=1;;
                            else
                                Zaehler:=2;;
                            fi;
                        od;
                    else
```

Abbildung 7:

```
                    continue;
                fi;
                if Zaehler=2 then
                    Zaehler:=0;;
                fi;
            fi;
        od;
    fi;
    if Zaehler<>1 then
        Print("alpha=",a,",beta=",b,",A=",d,",B=",e,",C=",f,"\n");
        SearchSol(d,e,f);
        Print("alpha=",a,",beta=",b,",A=",d,",B=",e,",C=",f,",xi=",xi,",eta=",eta,",zeta=",zeta,"\n");
        if Stop=0 then
            tSuche(a,b,d,e,f,xi,eta,zeta);
        else
            Stop:=0;;
            Print("Basisloesungen zu gross","\n");
        fi;
    fi;
fi;
fi;
fi;
fi;

if a * a + 2 * (b + 2) * (b + 2) <= 2000 then
   b := b + 2;
else
   a := a + 2;;
   c := a;;
   b := -30;;
   if a * a + 2 * b * b > 2000 then
      while a * a + 2 * b * b > 2000 do
         if 2 * b * b <=2000 then
            b:= b+2;
         else
            a:=0;;
            b:=0;;
         fi;
      od;
   fi;
   a := c;
fi;
od;
end;
```

Abbildung 8:

```
Try '?help' for help. See also '?copyrig
gap> Loesungssuche(1,-70);
alpha=1,beta=0,A=1,B=0,C=1
alpha=5,beta=-44,A=4337,B=-440,C=-3847
alpha=5,beta=12,A=193,B=120,C=-263
alpha=15,beta=-8,A=593,B=-240,C=97
alpha=25,beta=48,A=2833,B=2400,C=-3983
alpha=39,beta=-40,A=7841,B=-3120,C=-1679
alpha=45,beta=-4,A=2417,B=-360,C=1993
alpha=65,beta=-48,A=15073,B=-6240,C=-383
alpha=65,beta=-32,A=10433,B=-4160,C=2177
alpha=75,beta=-44,A=16097,B=-6600,C=1753
alpha=91,beta=-20,A=12721,B=-3640,C=7481
alpha=91,beta=20,A=5441,B=3640,C=7481
alpha=99,beta=-4,A=10625,B=-792,C=9769
alpha=99,beta=4,A=9041,B=792,C=9769
gap>
```

Abbildung 9: Mögliche Quadriken zur Lösung von 23 mit $\alpha^2 + 2\beta^2 \leq 10000$