Kapitel 9
Die Fermat-Vermutung für Zahlen und für Polynome

§1: Zahlen und Funktionen

Zum Beweis der eindeutigen Primzerlegung in der Hauptordnung eines Zahlkörpers mußten wir nur nachweisen, daß diese ein EUKLIDischer Ring ist, denn wie wir aus Kapitel 6, §5 wissen, ist jeder EUKLIDische Ring faktoriell. Da der Polynomring in einer Veränderlichen über einem Körper EUKLIDisch ist, gilt also auch dort das Gesetz von der eindeutigen Primzerlegung, wobei die irreduziblen Polynome die Rolle der Primzahlen einnehmen.

Besonders einfach ist die Situation, wenn der Grundkörper k algebraisch abgeschlossen ist: Dann hat jedes nichtkonstante Polynom $f \in k[x]$ eine Nullstelle a und ist damit durch $x - a$ teilbar. In diesem Fall sind also alle irreduziblen Polynome linear.

Die Zerlegung in irreduzible Elemente ist bekanntlich nur eindeutig bis auf Einheiten, und die Einheiten eines Polynomrings sind nach §1 aus Kapitel 6 gerade die des Koeffizientenrings, hier also die von Null verschiedenen Elemente von k. Durch Multiplikation mit einem solchen Element kann man den höchsten Koeffizienten eines jeden Polynoms zu eins machen; die irreduziblen Polynome über einem algebraisch abgeschlossenen Körper sind also bis auf Assoziiertheit genau die Polynome der Form $x - a$ mit $a \in k$ und sie entsprechen eindeutig den Elementen von k.

Den Primzahlen von $\mathbb{Z}$ entsprechen daher im Polynomring über einem algebraisch abgeschlossenen Körper die Punkte der affinen Geraden über k, wir können also geometrisch argumentieren.

Natürlich gibt es – zum Teil beträchtliche – Unterschiede zwischen $\mathbb{Z}$ und dem Polynomring über einem Körper, aber gerade das macht die Analogie so interessant: Da es für jeden der beiden Ringe ein eigenes Instrumentarium gibt, kann man versuchen die damit bewiesenen Resultate auf den jeweils anderen Fall zu übertragen, was idealerweise zu neuen Sätzen und sonst zumindest zu interessanten Vermutungen führt.

Als Beispiel für Parallelen und Unterschiede zwischen den beiden Situationen wollen wir die FERMAT-Vermutung betrachten. FERMAT schrieb bekanntlich um 1637 an den Rand seiner Arithmetik des DIOPHANTOS von Alexandrien, daß die Gleichung

$$x^n + y^n = z^n$$

für $n \geq 3$ keine Lösung in ganzen Zahlen habe – außer natürlich den trivialen Lösungen, bei denen eine der beiden Variablen verschwindet. (Die französische Übersetzung der Arithmetik, die er dabei benutzte, stammt übrigens von BACHET DE MÉZIRIAC, denn wir bereits als Entdecker des erweiterten EUKLIDischen Algorithmus kennen. Bekannt wurde FERMATs Randbemerkung erst, als dessen Sohn CLÉMENT-SAMUEL DE FERMAT 1670 die Arithmetik mit den Randbemerkungen seines fünf Jahre zuvor gestorbenen Vaters veröffentlichte.)

Es ist nicht möglich, einen Kubus in zwei Kuben oder ein Biquadrat in zwei Biquadrate und ganz allgemein irgendeine der unendlich vielen Potenzen jenseits des Quadrats in zwei ebensolche zu teilen. Ich habe einen wunderbaren Beweis hierfür gefunden, aber der Rand ist zu schmal, um ihn zu fassen.

Die direkte Verallgemeinerung auf Polynomringe ist sicherlich falsch: Die Gleichung $f^n + g^n = h^n$ ist zumindest für *konstante* Polynome über einem algebraisch abgeschlossenen Körper immer lösbar: Für beliebig vorgegebene Konstanten $f, g \in k$ muß man einfach $h = \sqrt[n]{f^n + g^n}$ setzen. Das sind allerdings, wenn wir uns wirklich für Polynome interessieren, uninteressante Lösungen, vergleichbar den Lösungen $x^n + 0^n = x^n$ der klassischen FERMAT-Gleichung.

Auch wenn wir verlangen, daß die Grade aller beteiligter Polynome positiv sein sollen, gibt es triviale Lösungen: Ist f irgendein beliebiges Polynom und sind $a, b, c \in k$ so, daß gilt $a^n + b^n = c^n$, ist natürlich auch $(af)^n + (bf)^n = (cf)^n$. Was wir höchstens erwarten können ist also das folgende Analogon zur klassischen FERMAT-Vermutung:

Für $n \geq 3$ gibt es keine paarweise teilerfremden Polynome f, g, h mit positivem Grad, so daß $f^n + g^n = h^n$ ist.

Für Körper positiver Charakteristik ist selbst das noch falsch: Über einen Körper der Charakteristik p ist schließlich $f^p + g^p = (f + g)^p$ für beliebige Polynome f und g, und dasselbe gilt auch wenn man den Exponenten p durch eine seiner Potenzen ersetzt. Wir können also höchstens für Körper der Charakteristik null erwarten, daß diese Vermutung für alle Exponenten $n \geq 3$ richtig ist, und genau das werden wir im übernächsten Paragraphen (zumindest für den Körper der komplexen Zahlen) auch beweisen. Zunächst aber wollen wir schauen, was im bei FERMAT ausgeschlossenen Fall des Exponenten zwei passiert.

§2: Pythagoräische Tripel

Betrachten wir zunächst den Fall der Polynome, wobei wir uns der Einfachheit halber gleich auf Polynome mit komplexen Koeffizienten beschränken wollen. Ist $f^2 + g^2 = h^2$, so ist

$$f^2 = h^2 - g^2 = (h + g)(h - g)\,.$$

Wenn wir f und g als teilerfremd voraussetzen, sind auch g und h teilerfremd und somit auch $h + g$ und $h - g$, denn jeder gemeinsame Teiler dieser beiden Polynome wäre auch ein Teiler ihrer Summe $2h$ sowie ihrer Differenz $2g$.

Wenn wir die Zerlegung von f^2 in irreduzible Faktoren vergleichen mit der von $h + g$ und $h - g$ folgt somit, daß jeder irreduzible Faktor von f entweder in $h + g$ oder in $h - g$ in gerader Potenz auftreten muß. Da jede komplexe Zahl ein Quadrat ist, können wir auch eine eventuell auftretende Einheit als Quadrat schreiben; somit gibt es zwei Polynome $u, v \in \mathbb{C}[x]$ derart, daß

$$u^2 = h + g, \quad v^2 = h - g \quad \text{und} \quad uv = f$$

ist, d.h.

$$f = uv, \quad g = \frac{u^2 - v^2}{2} \quad \text{und} \quad h = \frac{u^2 + v^2}{2}\,.$$

Starten wir umgekehrt mit zwei beliebigen teilerfremden Polynomen $u, v \in \mathbb{C}[x]$, erhalten mit Hilfe dieser Formeln Lösungen der Gleichung $f^2 + g^2 = h^2$. Damit kennen wir alle teilerfremden Lösungen, und die restlichen erhalten wir, indem wir alle drei Polynome mit einem gemeinsamen Faktor multiplizieren.

Nehmen wir als ein einfaches Beispiel $u = 2x$ und $v = 2$, ist also

$$f = 4x, \quad g = x^2 - 1 \quad \text{und} \quad h = x^2 + 1\,;$$

in der Tat ist

$$(2x)^2 + \left(x^2 - 1\right)^2 = \left(x^2 + 1\right)^2 .$$

Hier erhalten wir also mit geringem Aufwand eine vollständige Übersicht über alle Lösungen.

Versuchen wir das gleiche auch für den klassischen Fall! Wegen des Satzes von PYTHAGORAS bezeichnet man ein Tripel (x, y, z) ganzer Zahlen mit $x^2 + y^2 = z^2$ als pythagoräisches Tripel; für jedes solche Tripel gibt es ein rechtwinkliges Dreieck mit Seitenlängen $|x|, |y|$ und $|z|$.

Wir bezeichnen das Tripel (x, y, z) als *primitiv,* wenn sie sich nicht als Vielfaches eines anderen schreiben läßt, wenn also die Zahlen x, y, z keinen gemeinsamen Teiler haben. Sobald wir alle primitiven Lösungen kennen, können wir daraus die gesamte Lösungsmenge konstruieren, denn jede nichtprimitive Lösung ist Vielfaches einer primitiven.

Wie im Fall der Polynome gehen wir aus von einem primitiven Tripel (x, y, z) und wenden die dritte binomische Formel an:

$$x^2 = z^2 - y^2 = (z + y)(z - y)\,.$$

Hier können wir leider nicht mehr ohne weiteres folgern, daß $z + y$ und $z - y$ teilerfremd und damit Quadrate sind: Sind y und z beide ungerade, so sind ihre Summe und ihre Differenz beide gerade, also durch zwei teilbar. Wir müssen uns also zunächst über die Paritäten von y und z klarwerden.

Für eine primitive Lösung (x, y, z) müssen bereits x und y teilerfremd sein, denn ist d ein gemeinsamer Teiler von x und y, so sind x^2 und y^2

beide durch d^2 teilbar, also auch ihre Summe z^2. Wegen der eindeutigen Zerlegbarkeit einer natürlichen Zahl in Primfaktoren ist dann auch z durch d teilbar, d.h. d ist ein gemeinsamer Teiler von x, y und z.

Insbesondere können daher x und y nicht beide gerade sein; mindestens eine der beiden Zahlen muß ungerade sein. Andererseits können aber auch nicht beide Zahlen ungerade sein: Wäre nämlich $x = 2u + 1$ und $y = 2v + 1$, so wäre

$$z^2 = (2u + 1)^2 + (2v + 1)^2 = 4u^2 + 4u + 1 + 4v^2 + 4v + 1 \equiv 2 \bmod 4\,,$$

was unmöglich ist, da modulo vier nur null und eins Quadrate sind.

Somit muß in einem primitiven pythagoräischen Tripel (x, y, z) eine der beiden Zahlen x, y gerade sein und die andere ungerade. Da mit (x, y, z) auch (y, x, z) ein primitives pythagoräisches Tripel ist, genügt es, wenn wir diejenigen Tripel betrachten, in denen x gerade ist und y ungerade. Offensichtlich ist dann auch z ungerade.

Für so ein Tripel steht in der Gleichung

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$

rechts das Produkt zweier gerader Zahlen. Im Gegensatz zur Situation bei den Polynomen haben wir hier also keine teilerfremden Faktoren.

Dividieren wir aber durch zwei, so können wir wie oben argumentieren, daß $\frac{1}{2}(z+y)$ und $\frac{1}{2}(z-y)$ teilerfremd sind, denn jeder gemeinsame Teiler wäre Teiler ihrer Summe z und ihrer Differenz y.

Jetzt können wir wieder die eindeutige Primzerlegung anwenden: Da

$$x^2 = 2^2 \cdot \left(\frac{z + y}{2}\right) \cdot \left(\frac{z - y}{2}\right)\,,$$

wobei die beiden Klammern teilerfremd sind, gibt es ganze Zahlen u, v, so daß

$$u^2 = \left(\frac{z + y}{2}\right), \quad v^2 = \left(\frac{z + y}{2}\right) \quad \text{und} \quad 2uv = x$$

ist, also

$$x = 2uv, \quad y = u^2 - v^2 \quad \text{und} \quad z = u^2 - v^2\,.$$

Umgekehrt definieren diese Formeln für beliebige ganze Zahlen u und v ein primitives pythagoräisches Tripel, und bis auf die Reihenfolge von x und y erhalten wir so auch jedes dieser Tripel, für $u = 2$ und $v = 1$ etwa das seit Jahrtausenden bekannte Tripel $(4, 3, 5)$. Da sich in alten Sakralbauten und -anlagen auch deutlich kompliziertere pythagoräische Tripel nachweisen lassen, steht zu vermuten, daß die obige Konstruktion möglicherweise bereits in einigen steinzeitlichen Kulturen zumindest teilweise bekannt waren; entsprechende Thesen vertritt beispielsweise bekannte algebraische Geometer B.L. VAN DER WAERDEN (1903–1996), der nach seiner Emeritierung auch mehrere Bücher über die Geschichte der Mathematik veröffentlichte. Mit pythagoräischen Tripel beschäftigt er sich ausführlich in

B.L. VAN DER WAERDEN: Geometry and algebra in ancient civilizations, *Springer*, 1983

§3: Der Satz von Mason

In diesem Abschnitt wollen wir, wie bereits angekündigt, sehen, daß es für $n \geq 3$ keine zueinander teilerfremden Polynome positiven Grades $f, g, h \in \mathbb{C}[x]$ gibt mit $f^n + g^n = h^n$.

Der *Beweis* beruht darauf, daß die Polynome f^n und g^n dieselben Nullstellen wie f und g haben, aber mit n-facher Vielfachheit. Ist $f^n + g^n = h^n$, so hat auch die Summe dieser beiden Potenzen im Vergleich zum Grad relativ wenige Nullstellen, diese aber mit mindestens n-facher Vielfachheit. Nach einem 1983 von R.C. MASON bewiesenen Satz können in einer solchen Situation aber f^n, g^n und h^n nicht zu wenige verschiedene Nullstellen haben:

Satz: Bezeichnet $n_0(f)$ die Anzahl verschiedener (komplexer) Nullstellen eines Polynoms f, so gilt für drei nichtkonstante, teilerfremde Polynome f, g, h mit $f + g = h$

$$n_0(fgh) \geq \max(\deg f, \deg g, \deg h) + 1 \,.$$

Bevor wir diesen Satz beweisen, wollen wir uns zunächst überlegen, daß daraus wirklich die FERMAT-Vermutung für Polynome folgt:

Für drei nichtkonstante teilerfremde Polynome f, g, h mit $f^n + g^n = h^n$ ist nach dem Satz von MASON

$$\begin{aligned} n_0\big(f^n g^n h^n\big) &\geq \max\big(\deg f^n, \deg g^n, \deg h^n\big) + 1 \\ &= n \max\big(\deg f, \deg g, \deg h\big) + 1 \,. \end{aligned}$$

Andererseits ist aber

$$\begin{aligned} n_0\big(f^n g^n h^n\big) &= n_0\big(fgh\big) \\ &\leq \deg f + \deg g + \deg h \\ &\leq 3 \max\big(\deg u(x), \deg v(x), \deg w(x)\big) \,, \end{aligned}$$

denn die Anzahl *verschiedener* Nullstellen einer Potenz eines Polynoms ist gleich der Anzahl verschiedener Nullstellen des Polynoms selbst, und die Nullstellenanzahl eines Polynom kann nicht größer sein als der Grad.

Damit haben wir insgesamt die Ungleichung

$$\begin{aligned} 3 \max\big(\deg f, \deg g, \deg h\big) &\geq n_0\big(f^n g^n h^n\big) \\ &\geq n \max\big(\deg f, \deg g, \deg h\big) + 1 \,, \end{aligned}$$

die bei nichtkonstanten Polynomen nur für $n \leq 2$ gelten kann. Somit gibt es für $n \geq 3$ keine nichtkonstanten teilerfremden Polynome, für die $f^n + g^n = h^n$ ist.

Zu einem vollständigen Beweis der FERMAT-Vermutung für Polynome fehlt nun nur noch der Beweis des Satzes von MASON. Die Idee dazu ist folgende: Ist $f + g = h$, so betrachten wir den Quotienten g/f im rationalen Funktionenkörper $\mathbb{C}(x)$. Da f und g teilerfremd sind, ist das ein gekürzter Bruch. Falls wir diesen auch in der Form $g/f = G/F$ schreiben können mit Polynomen F, G vom Grad höchstens $n_0(fgh) - 1$ schreiben können, so haben auch f und g höchstens den Grad $n_0(fgh) - 1$. Wegen $f + g = h$ gilt dasselbe auch für h, und damit wäre der Satz bewiesen.

Um g/f als Quotienten zweier neuer Polynome auszudrücken, schreiben wir zunächst

$$\frac{g}{f} = \frac{S}{R} \quad \text{mit} \quad R = \frac{f}{h} \;\text{ und }\; S = \frac{g}{h} \,.$$

Dabei ist $R + S = 1$, die Summe $R' + S'$ der Ableitungen verschwindet also. Aus der Gleichung

$$R' + S' = \frac{R'}{R}R + \frac{S'}{S}S$$

folgt die neue Darstellung

$$\frac{g}{f} = \frac{S}{R} = -\frac{R'/R}{S'/S}\,.$$

Rechts stehen die logarithmischen Ableitungen von R und S im Zähler und Nenner, und damit lassen sich gut die Nullstellen von f, g und h ins Spiel bringen: Nach der LEIBNIZ-Regel ist bekanntlich

$$(uv)' = u'v + uv', \quad \text{also} \quad \frac{(uv)'}{uv} = \frac{u'}{u} + \frac{v'}{v}\,,$$

die logarithmische Ableitung eines Produkts ist also einfach die Summe der logarithmischen Ableitungen der Faktoren. Daraus folgt sofort, daß die logarithmische Ableitung eines Quotienten gleich der Differenz aus logarithmischer Ableitung des Zählers und logarithmischer Ableitung des Nenners ist. Schreiben wir

$$f = f_0 \prod_{i=1}^{r}(x-a_i)^{n_i}, \quad g = g_0 \prod_{j=1}^{s}(x-b_j)^{s_j} \quad \text{und} \quad h = h_0 \prod_{k=1}^{t}(x-c_k)^{p_k}\,,$$

so ist also

$$\frac{R'}{R} = \frac{f'}{f} - \frac{h'}{h} = \sum_{i=1}^{r}\frac{n_i}{x-a_i} - \sum_{k=1}^{t}\frac{p_k}{x-c_k}\,,$$

$$\frac{S'}{S} = \frac{g'}{g} - \frac{h'}{h} = \sum_{j=1}^{r}\frac{m_j}{x-b_j} - \sum_{k=1}^{t}\frac{p_k}{x-c_k}$$

$$\text{und} \quad \frac{g}{f} = \frac{R'/R}{S'/S} = -\,\frac{\displaystyle\sum_{i=1}^{r}\frac{n_i}{x-a_i} - \sum_{k=1}^{t}\frac{p_k}{x-c_k}}{\displaystyle\sum_{j=1}^{s}\frac{m_j}{x-b_j} - \sum_{k=1}^{t}\frac{p_k}{x-c_k}}\,.$$

Erweitern wir Zähler und Nenner mit dem Hauptnenner aller Summanden erweitern, d.h. mit dem Polynom vom Grad $r + s + t = n_0(fgh)$

$$H = \prod_{i=1}^{r}(x - a_i) \cdot \prod_{j=1}^{s}(x - b_j) \cdot \prod_{k=1}^{t}(x - c_k)\,,$$

so erhalten wir im Zähler wie auch im Nenner Summen von Polynomen vom Grad $n_0(fgh) - 1$, als Polynome vom Grad höchstens $n_0(fgh) - 1$, wie gewünscht. Damit ist der Satz von MASON bewiesen.

§4: Die abc-Vermutung

Der Erfolg des Satzes von MASON beim Beweis der FERMAT-Vermutung für Polynome legt es nahe, etwas ähnliches auch im klassischen Fall zu versuchen.

Da natürliche Zahlen weder Grade noch Nullstellen haben, müssen wir dazu den Satz von MASON zunächst einmal so umformulieren, daß wir eine Aussage bekommen, die ein sinnvolles Analogon für natürliche Zahlen hat.

Dazu ordnen wir einem Polynom f anstelle der Anzahl $n_0(f)$ seiner (verschiedenen) Nullstellen ein *Polynom* $N_0(f)$ dazu, das genau diese Nullstellen mit jeweils der Vielfachheit eins haben soll: Für

$$f = f_0 \prod_{i=1}^{r}(x - a_i)^{n_i} \quad \text{sei} \quad N_0(f) \underset{\text{def}}{=} \prod_{i=1}^{r}(x - a_i)\,,$$

so daß der Grad von $N_0(f)$ gerade die im vorigen Paragraphen definierte Zahl $n_0(f)$ ist.

Der Vorteil des Polynoms $N_0(f)$ besteht darin, daß wir eine analoge Definition leicht auch für natürliche Zahlen hinschreiben können: Für

$$n = \prod_{i=1}^{r} p_i^{e_i} \quad \text{setzen wir} \quad N_0(n) \underset{\text{def}}{=} \prod_{i=1}^{r} p_i\,.$$

Mit Hilfe der Polynome $N_0(f)$ läßt sich der Satz von MASON folgendermaßen umformulieren:

Gilt für drei teilerfremde Polynome f, g und h die Gleichung $f + g = h$, so hat jedes der drei Polynome einen kleineren Grad als das Polynom $N_0(fgh)$.

In dieser Formulierung kommt immer noch der Grad vor, für den wir bei natürlichen Zahlen keine Verwendung haben. Betrachten wir aber den Grad lediglich als eine Methode, einem Polynom eine Zahl aus $\mathbb{N}_0$ zuzuordnen, so können wir, wenn wir bereits natürliche Zahlen haben, einfach ganz auf ihn verzichten; falls wir ganze Zahlen betrachten, liegt es nahe, ihn durch den Betrag zu ersetzen.

Gemäß dieser Philosophie können wir nun probeweise die folgende Aussage formulieren:

A1: *Ist $c = a+b$ für drei zueinander teilerfremde natürliche Zahlen a, b, c, so ist jede der drei Zahlen kleiner als $N_0(abc)$.*

Damit haben wir eine sinnvolle Aussage über natürliche Zahlen gefunden, die – falls sie korrekt ist – sofort die FERMAT-Vermutung impliziert: Gibt es nämlich drei natürliche Zahlen x, y, z mit der Eigenschaft, daß $x^n + y^n = z^n$ für ein $n \geq 3$, so gibt es auch drei zueinander teilerfremde Zahlen x, y, z mit dieser Eigenschaft: Wir müssen einfach die drei Zahlen durch ihren größten gemeinsamen Teiler kürzen. Alsdann muß, falls obige Aussage richtig ist, jede der drei Potenzen x^n, y^n, z^n kleiner sein als $N_0(x^n y^n z^n)$. Nun ist aber

$$N_0(x^n y^n z^n) = N_0(xyz) \leq xyz\,,$$

d.h. jede der drei Zahlen x^n, y^n, z^n wäre kleiner als xyz. Damit wäre

$$(xyz)^n = x^n y^n z^n < (xyz)^3\,,$$

was für $n \geq 3$ offensichtlich nicht möglich ist.

Angesichts der Komplexität des WILESschen Beweises fällt es schwer, an einen so einfachen Beweis zu glauben, und in der Tat ist die obige Aussage in dieser Form falsch:

Betrachten wir etwa die Gleichung $8 + 1 = 9$. Offensichtlich sind die drei Summanden teilerfremd zueinander, aber sowohl 8 als auch 9 sind größer als $N_0(8 \cdot 1 \cdot 9) = 2 \cdot 3 = 6$. Ganz so einfach geht es also nicht.

Da der Grad eines Polynoms nicht durch konstante Faktoren beeinflußt wird, könnte man versuchen, als „richtiges“ Analogon zum Satz von MASON eine abgeschwächte Aussage zu nehmen, die nur eine Abschätzung bis auf einen konstanten Faktor enthält, etwa

A2: *Ist $c = a+b$ für drei zueinander teilerfremde natürliche Zahlen a, b, c, so gibt es eine Konstante K derart, daß jede der drei Zahlen kleiner ist als $K \cdot N_0(abc)$.*

Diese Aussage ist trivialerweise richtig: Wir müssen nur eine Konstante K wählen, die größer ist als das Maximum von a, b und c. Leider ist sie auch völlig nutzlos, denn solange die Konstante von a, b und c abhängen darf, haben wir keine Chance, damit die FERMAT-Vermutung zu beweisen.

Wir müssen die Aussage also noch einmal umformulieren:

A3: *Es gibt eine Konstante K, so daß gilt: Ist $c = a+b$ für drei zueinander teilerfremde natürliche Zahlen a, b, c, so ist jede der drei Zahlen kleiner als $K \cdot N_0(abc)$.*

Wie wir gleich sehen werden, würde hieraus die FERMAT-Vermutung zumindest für alle hinreichend großen Exponenten n folgen, allerdings ist die Aussage, so wie sie dasteht, leider immer noch falsch:

Betrachten wir die Gleichung

$$a_n + b_n = c_n \quad \text{mit} \quad a_n = 3^{2^n} - 1, \quad b_n = 1 \quad \text{und} \quad c_n = 3^{2^n}. \quad (*)$$

Wäre sie richtig, müßte für jedes n gelten:

$$3^{2^n} \leq K N_0\big((3^{2^n} - 1)3^{2^n}\big) = K \cdot 3 \cdot N_0(3^{2^n} - 1)\,.$$

Um $N_0(3^{2^n} - 1)$ abzuschätzen, beachten wir, daß gilt

$$3^{2^n} = \big(3^{2^{n-1}}\big)^2 \quad \text{und} \quad 3^{2^n} - 1 = \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-1}} - 1\big)$$

nach der dritten binomischen Formel. Wenden wir dies mehrfach an,

erhalten wir

$$\begin{aligned} 3^{2^n} - 1 &= \left(3^{2^{n-1}} + 1\right)\left(3^{2^{n-1}} - 1\right) \\ &= \left(3^{2^{n-1}} + 1\right)\left(3^{2^{n-2}} + 1\right)\left(3^{2^{n-2}} - 1\right) \\ &= \left(3^{2^{n-1}} + 1\right)\left(3^{2^{n-2}} + 1\right)\left(3^{2^{n-3}} + 1\right)\left(3^{2^{n-3}} - 1\right) \\ &= \dots \\ &= \left(3^{2^{n-1}} + 1\right)\left(3^{2^{n-2}} + 1\right) \dots \left(3^2 + 1\right)\left(3^1 + 1\right)\left(3^1 - 1\right). \end{aligned}$$

In der letzten Zeile steht ein Produkt aus $n+1$ geraden Zahlen; somit ist $3^{2^n} - 1$ durch 2^{n+1} teilbar. Das Produkt $N_0(3^{2^n} - 1)$ aller *verschiedener* Primteiler von $3^{2^n} - 1$ erfüllt daher die Ungleichung

$$N_0(3^{2^n} - 1) \leq 2 \cdot \frac{3^{2^n} - 1}{2^{n+1}} = \frac{3^{2^n} - 1}{2^n},$$

denn das Produkt aller ungerader Primteiler kann höchstens gleich $(3^{2^n} - 1)/2^n$ sein.

Falls **A3** korrekt wäre, müßte nach Gleichung $(*)$ also gelten

$$3^{2^n} \leq \frac{3K}{2^n}(3^{2^n} - 1) \quad \text{für alle } n\,.$$

Das kann aber unmöglich der Fall sein, denn für hinreichend große n ist der Faktor $\frac{3K}{2^n}$ kleiner als eins, so daß 3^{2^n} echt kleiner als sich selbst sein müßte.

Auf der Suche nach einem Analogon für den Satz von MASON müssen wir daher noch weiter abschwächen. *Eine* Möglichkeit dazu ist die 1986 aufgestellte

abc-Vermutung von MASSER und OESTERLÉ: Zu jedem $\varepsilon > 0$ gibt es eine Konstante $K(\varepsilon)$, so daß für alle teilerfremden natürlichen Zahlen a, b, c mit $a+b=c$ gilt: Jede der drei Zahlen a, b, c ist kleiner oder gleich $K(\varepsilon) \cdot N_0(abc)^{1+\varepsilon}$.

Diese Vermutung ist, im Gegensatz zur FERMAT-Vermutung, bis heute offen.

Wir wollen uns überlegen, daß sie zumindest für große Exponenten n die FERMAT-Vermutung impliziert.

Dazu betrachten wir eine Lösung $x^n + y^n = z^n$ mit o.B.d.A. teilerfremden natürlichen Zahlen x, y, z und wählen uns irgendein $\varepsilon > 0$. Nach der abc-Vermutung gibt es dazu eine Konstante $K(\varepsilon)$, so daß x^n, y^n und z^n allesamt höchstens gleich

$$K(\varepsilon)N_0(x^n y^n z^n)^{1+\varepsilon} = K(\varepsilon)N_0(xyz)^{1+\varepsilon} \leq K(\varepsilon)(xyz)^{1+\varepsilon}$$

sind. Für ihr Produkt gilt daher

$$x^n y^n z^n \leq K(\varepsilon)^3 (xyz)^{3(1+\varepsilon)} \quad \text{oder} \quad (xyz)^{n-3-3\varepsilon} \leq K(\varepsilon)^3 .$$

$K(\varepsilon)^3$ ist eine feste Zahl; es gibt daher einen Exponenten m derart, daß $2^m > K(\varepsilon)^3$ ist. Da das Produkt xyz auf jeden Fall nicht kleiner als zwei sein kann, ist dann für $n - 3 - 3\varepsilon > m$ oder $n > m + 3 + 3\varepsilon$ insbesondere

$$(xyz)^{n-3-3\varepsilon} > K(\varepsilon)^3 .$$

Für Exponenten $n > m + 3 + 3\varepsilon$ kann daher die FERMAT-Gleichung keine Lösung in natürlichen Zahlen haben.

Ob und gegebenenfalls welche konkreten Schranken für n man damit erreichen kann, hängt natürlich davon ab, wie $K(\varepsilon)$ von ε abhängt. Dazu gibt es im Augenblick nicht einmal Vermutungen.

Für weitere Informationen zu §3 und §4 sei auf einen Vortrag verwiesen, den SERGE LANG in Zürich vor einem „allgemeinen“ Publikum hielt und dem ich hier im wesentlichen gefolgt bin:

SERGE LANG: Die abc-Vermutung, *Elemente der Mathematik* **48** (1993), 89-99

Der Artikel ist (wie die gesamte Zeitschrift *Elemente der Mathematik)* unter `http://www.bibliothek.uni-regensburg.de/ezeit/?2135837` frei zugänglich.

§5: Die Frey-Kurve

Da die FERMAT-Vermutung seit 1994 bewiesen ist, die abc-Vermutung aber immer noch offen, mußte der Beweis der FERMAT-Vermutung

natürlich andere Wege gehen. Die meisten dieser Wege führen in Gebiete, die weit jenseits dessen liegen, was selbst ein guter auf Zahlentheorie spezialisierter Diplom-Mathematiker im Laufe seines Studiums lernen kann, aber zumindest die Grundidee der abc-Vermutung, daß man nämlich Summenbeziehungen zwischen großen Zahlen nicht ohne ein gewisses Minimum an verschiedenen Primfaktoren realisieren kann, spielt in modifizierter Weise in der Tat eine große Rolle.

Der Anstoß kam 1984 von GERHARD FREY, damals Professor an der Universität Saarbrücken, wo er auf dem Gebiet der Arithmetik elliptischer Kurven arbeitete. Heute leitet er die Arbeitsgruppe Zahlentheorie am Institut für experimentelle Mathematik der (inzwischen mit Duisburg vereinigten) Universität Essen und beschäftigt sich mit der Anwendung elliptischer (und anderer) Kurven in der Kryptologie.

Elliptische Kurven sind ebene Kurven, die durch eine Gleichung der Form $y^2 = f_3(x)$ beschrieben werden mit einem Polynom $f_3(x)$ vom Grad drei mit drei verschiedenen Nullstellen. Da das Quadrat einer reellen Zahl nicht negativ sein kann, gibt es im Reellen nur Punkte mit x-Koordinaten, für die $f_3(x) \geq 0$ ist. Im Falle $f_3(x) > 0$ erfüllt mit y auch $-y$ die obige Gleichung, die Kurve ist also symmetrisch zur x-Achse.

Falls $f_3(x)$ nur zwei verschiedene Nullstellen hat, muß eine der Nullstellen doppelt sein, und bei diesem x-Wert überkreuzt sich die Kurve; wir reden dann von einer Knotenkurve.

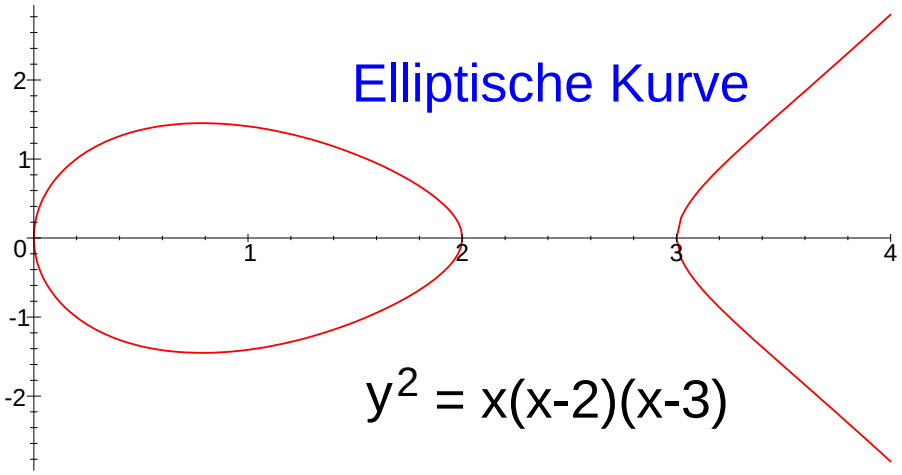
Hat schließlich $f_3(x)$ nur eine, dafür aber dreifache Nullstelle, entsteht eine Spitzenkurve.

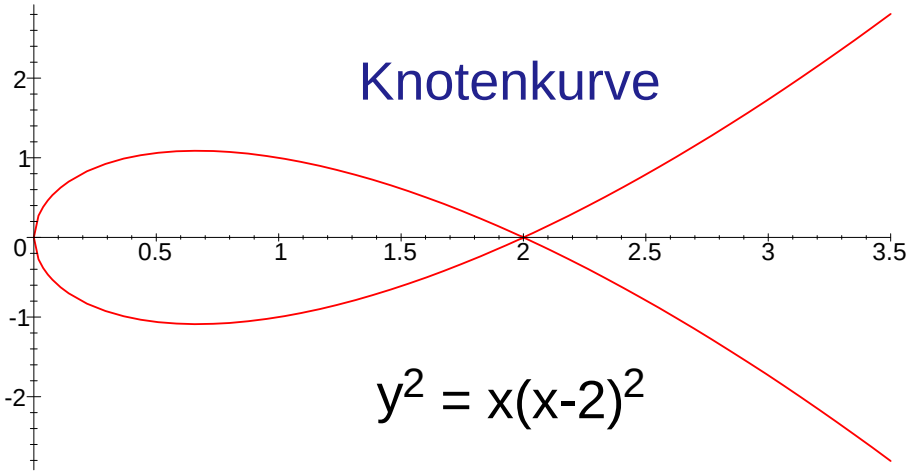
FREY betrachtete eine (hypothetische) Lösung

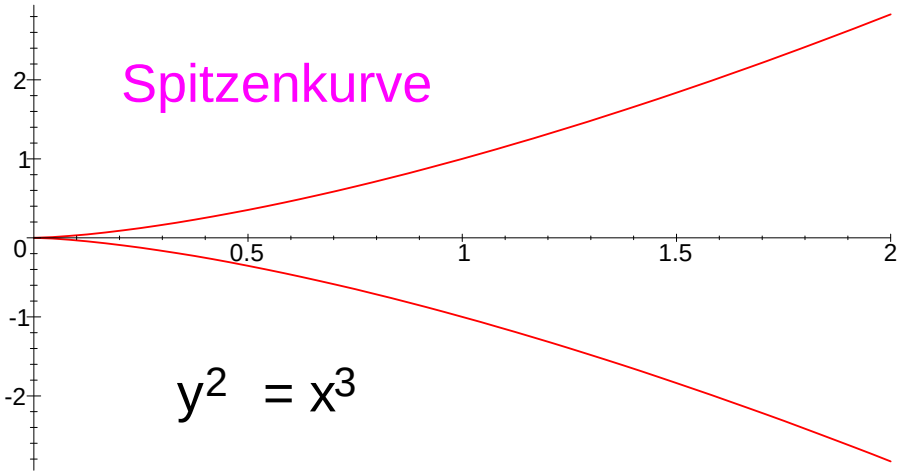
$$x^n + y^n = z^n$$

der FERMAT-Gleichung mit teilerfremden natürlichen Zahlen x, y, z und $n \geq 5$. (Den Fall $n = 4$ hat, wie wir gesehen haben, bereits FERMAT selbst gelöst, den Fall $n = 3$ nicht viel später EULER.) Wenn es eine solche Lösung gibt, dann gibt es auch eine Lösung für einen Primzahlexponenten ℓ, denn ist ℓ ein Primteiler von n und $n = \ell m$, so ist auch

$$a^\ell + b^\ell = c^\ell \quad \text{mit} \quad a = x^m, \quad b = y^m \quad \text{und} \quad c = z^m$$


Elliptische Kurve
$y^2 = x(x-2)(x-3)$


Knotenkurve
$y^2 = x(x-2)^2$


Spitzenkurve
$y^2 = x^3$

eine Lösung, und auch a, b, c sind teilerfremd. Auch für ℓ genügt es, den Fall $\ell \geq 5$ zu betrachten, denn wenn wir für ℓ den größten Primteiler von n nehmen, bedeutet $\ell = 2$, daß n eine Zweierpotenz sein muß, was für $n = 2$ kein Widerspruch zur FERMAT-Vermutung ist und für $n = 4$ und damit auch jede höhere Zweierpotenz nach FERMATs Beweis ausgeschlossen ist. Für den Fall $\ell = 3$ kann wieder auf EULER verwiesen werden.

Zur obigen Lösung definiert FREY die elliptische Kurve

$$y^2 = x(x - a^\ell)(x + b^\ell)$$

zu, die er aber nicht nur über den reellen oder komplexen Zahlen betrachtet, sondern auch über den ganzen Zahlen modulo einer Primzahl p:

Ist allgemein

$$y^2 = (x - x_1)(x - x_2)(x - x_3)$$

eine Kurvengleichung mit ganzen Zahlen x_1, x_2, x_3, so können wir für x und y auch ganze Zahlen einsetzen und diese Gleichung modulo p betrachten. Wir sprechen wieder von einer elliptischen Kurve, einer Knotenkurve oder einer Spitzenkurve je nachdem wie viele der Nullstellen x_1, x_2 und x_3 modulo p noch verschieden sind.

Die obige Gleichung definiert genau dann eine elliptische Kurve, wenn alle drei Nullstellen verschieden sind, wenn also die sogenannte Diskriminante

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

von Null verschieden ist. Modulo p definiert sie eine elliptische Kurve, wenn Δ auch modulo p noch von Null verschieden ist, wenn also p kein Teiler von Δ ist.

Speziell für die FREY-Kurve $y^2 = x(x-a^\ell)(x+b^\ell)$ ist die Diskriminante

$$\Delta = (0 - a^\ell)(0 - b^\ell)\left(a^\ell - (-b)^\ell\right) = a^\ell b^\ell (a^\ell + b^\ell) = a^\ell b^\ell c^\ell = (abc)^\ell$$

stets von Null verschieden; modulo p verschwindet sie genau dann, wenn p ein Teiler von Δ ist, d.h., wenn p eine der drei Zahlen a, b, c teilt.

Da die Diskriminante als ℓ-te Potenz von abc verglichen mit a, b, c ziemlich groß ist, heißt das, daß es im Verhältnis zur Größe der Diskriminante

erstaunlich wenige Primzahlen gibt, modulo derer wir *keine* elliptische Kurve erhalten; wir sind also wieder einer ähnlichen Situation wie bei der abc-Vermutung. Die FREYsche Kurve sieht damit so aus, als sei sie fast zu schön, um wirklich zu existieren.

Einen Anhaltspunkt zum Beweis dieser Nichtexistenz liefert eine Vermutung, die auf um 1955 durchgeführte Rechnungen und Spekulationen des japanischen Mathematikers TANIYAMA zurückgeht und heute je nach Autor mit irgendeiner Kombination der drei Namen TANIYAMA, SHIMURA und WEIL bezeichnet wird. Danach sollte es zu einer elliptischen Kurve E mit ganzzahligen Koeffizienten eine surjektive Abbildung $X_0(N) \to E$ von einer sogenannten Modulkurve $X_0(N)$ auf E geben, wobei N im wesentlichen das Produkt aller Primzahlen p ist, modulo derer E keine elliptische Kurve mehr ist. Wie FREYs Rechnungen zeigen, hat seine Kurve vor diesem Hintergrund sehr seltsame Eigenschaften.

Als er damals hier in Mannheim über seine Resultate vortrug, meinte er noch, er glaube nicht, daß die FERMAT-Vermutung so bewiesen werde; er veröffentlichte sein Ergebnis auch nicht in einer der großen internationalen Fachzeitschriften, sondern als Band 1, Heft 1 einer gerade neu gestarteten Schriftenreihe der Universität Saarbrücken, in einfachster Aufmachung xerographiert mit einem nur schwarz-weiß gestalteten Karton als Umschlag:

GERHARD FREY: Links between stable elliptic curves and certain diophantine equations, *Annales Universitatis Saraviensis, Series Mathematicae,* **1** *(1), 1986*

1987 verschärfte der französische Mathematiker JEAN-PIERRE SERRE die TANIYAMA-Vermutung, und aus dieser stärkeren Vermutung folgt in der Tat, daß die FREY-Kurve nicht existieren kann. Leider ist die SERREsche Vermutung bis heute noch nicht bewiesen.

SERRE erhielt übrigens 2002 den ersten der vom norwegischen Parlament gestifteten ABEL-Preise, die seither zur Erinnerung an den norwegischen Mathematiker NIELS HENRIK ABEL (1802–1829) jedes Jahr in gleicher Weise und gleicher Ausstattung wie die Nobel-Preise für hervorragende Leistungen auf dem Gebiet der Mathematik vergeben werden.

SERRE stellte jedoch noch zusätzlich seine sogenannte ε-Vermutung auf,

und auch aus der TANIYAMA-Vermutung zusammen mit der ε-Vermutung folgt die Nichtexistenz der FREY-Kurve und damit die FERMAT-Vermutung. Diese ε-Vermutung bewies KENNETH RIBET von der Universität Berkeley 1990. Die Grundidee seines Beweises läßt sich interpretieren als eine Art zweidimensionale Version eines Beweises von ERNST EDUARD KUMMER (1810–1893), der die FERMAT-Vermutung 1846 für sogenannte reguläre Primzahlen als Exponenten bewies. (Eine Primzahl p heißt regulär, wenn die Hauptordnung des Körpers $\mathbb{Q}[\zeta_p]$ der p-ten Einheitswurzeln faktoriell ist.) Der Beweis von RIBET ist allerdings erheblich aufwendiger.

Damit war also die FERMAT-Vermutung zurückgeführt auf die TANIYAMA-Vermutung. Diese Vermutung schließlich (die für die weitere mathematische Forschung erheblich wichtiger ist als die FERMAT-Vermutung) bewies WILES 1994.