Kapitel 5
Die Fermat-Vermutung für Zahlen und für Polynome

§1: Zahlen und Funktionen

Wir haben im Verlauf dieser Vorlesung zweimal einen Satz über eindeutige Primzerlegung bewiesen: Zuerst für den Ring $\mathbb{Z}$ der ganzen Zahlen, und später für Polynomringe über Körpern (oder allgemeiner über faktoriellen Ringen). Speziell im Falle von Polynomringen in einer Variablen über einem Körper war der Beweis praktisch identisch zu dem für die ganzen Zahlen; beide Male ging es darum, daß der Ring EUKLIDisch ist.

Die Rolle der Primzahlen spielten im Polynomring die irreduziblen Polynome. Im Falle eines algebraisch abgeschlossenen Körpers k sind das gerade die linearen Polynome, und die bilden im Gegensatz zu den Primzahlen eine sehr übersichtliche Menge. Da es auf konstante Faktoren nicht ankommt, kann man sich auf Polynome der Form $X - a$ mit $a \in k$ beschränken. Die Menge aller dieser Polynome wiederum kann identifiziert werden mit der Menge aller $a \in k$, deren Elemente man mit den Punkten einer Geraden identifizieren kann, so daß in einigen Anwendungen auch geometrische Argumente möglich sind.

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 drei Zahlen verschwindet. (Die französische Übersetzung der Arithmetik, die er dabei benutzte, stammt übrigens von BACHET DE MÉZIRIAC, denn wir als Entdecker des erweiterten EUKLIDischen Algorithmus kennen. Bekannt wurde FERMATs Randbemerkung erst, als sein 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 teilerfremden Polynome f, g, h mit positivem Grad, so daß $f^n + g^n = h^n$ ist.

(Normalerweise unterscheiden wir sorgfältig zwischen paarweise teilerfremden Polynomen und solchen, die nur insgesamt keinen gemeinsamen Teiler haben. Hier sind beide Begriffe äquivalent, da jeder gemeinsame Teiler zweier der Polynome f, g, h wegen $f^n + g^n = h^n$ auch das dritte teilen muß.)

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 nächsten Paragraphen zumindest für den Körper der komplexen Zahlen und damit auch jeden Teilkörper davon beweisen.

§2: Der Satz von Mason

Wir wollen zeigen, 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 $f, g, h \in \mathbb{C}[X]$ 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 das Analogon der 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

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

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

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

die nur für $n \le 2$ gelten kann. Somit gibt es für $n \ge 3$ 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 $n_0(fgh)-1$, haben auch Zähler und Nenner f und g des gekürzten Bruchs höchstens den Grad $n_0(fgh) - 1$. Wegen $f + g = h$ gilt dasselbe auch für h, und damit ist $n_0(fgh) - 1 \le \max(\deg f, \deg g, \deg h)$, was zur Aussage des Satzes äquivalent ist.

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

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

Wegen $f + g = h$ ist $R + S = 1$, die Summe $R' + S'$ der Ableitungen verschwindet also. Dies können wir etwas umschreiben

$$R' + S' = \frac{R'}{R}R + \frac{S'}{S}S = 0 \Longrightarrow \frac{R'}{R}R = -\frac{S'}{S}S \Longrightarrow \frac{R}{S} = -\frac{R'}{R}\Big/\frac{S'}{S}\,,$$

und damit erhalten wir 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

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

mit $f_0, g_0, h_0 \in \mathbb{C}^\times$, ist also wegen $R = \frac{f}{h}$ und $S = \frac{g}{h}$

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

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

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

Erweitern wir Zähler und Nenner mit dem Hauptnenner aller Summanden, 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 $n_0(fgh)-1$, also Polynome vom Grad höchstens $n_0(fgh)-1$, wie gewünscht. Damit sind sowohl der Satz von MASON als auch das Analogon der FERMATschen Vermutung für Polynome bewiesen.

§3: 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 (wie bei der Polynomdivision mit Rest) 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 a+b = c 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: Gäbe es nämlich drei natürliche Zahlen x, y, z mit der Eigenschaft, daß $x^n + y^n = z^n$ für ein $n \geq 3$, so gäbe 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 müßte, falls obige Aussage richtig wäre, 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. nach **A1** wäre jede der drei Zahlen x^n, y^n, z^n 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 Aussage **A1** 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 a+b = c 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, für die gilt: Ist a+b = c für drei zueinander teilerfremde natürliche Zahlen a, b, c, so ist jede der drei Zahlen kleiner als $K \cdot N_0(abc)$.*

Auch daraus würde 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:

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

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

$$\begin{aligned} 3^{2^n} - 1 &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-1}} - 1\big) \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} + 1\big)\big(3^{2^{n-2}} - 1\big) \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} + 1\big)\big(3^{2^{n-3}} + 1\big)\big(3^{2^{n-3}} - 1\big) \\ &= \cdots \\ &= \big(3^{2^{n-1}} + 1\big)\big(3^{2^{n-2}} + 1\big) \ldots \big(3^2 + 1\big)\big(3^1 + 1\big)\big(3^1 - 1\big)\,. \end{aligned}$$

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

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

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

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

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 $K(\varepsilon) \cdot N_0(abc)^{1+\varepsilon}$.

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

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

sind. Für ihr Produkt gilt daher

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

$K(\varepsilon)^3$ 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 $2^{n-3-3\varepsilon} < 2^m$, also $n - 3 - 3\varepsilon < m$ und $n < m + 3 + 3\varepsilon$. Für $n \geq m + 3 + 3\varepsilon$ ist daher

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

und damit kann es keine zueinander teilerfremden natürlichen Zahlen x, y, z geben mit $x^n + y^n = z^n$.

Ob und gegebenenfalls welche konkreten Schranken für n man damit erreichen kann, hängt natürlich davon ab, wie $K(\varepsilon)$ von ε abhängt. Nach einigen Spekulationen könnte aus der abc-Vermutung die FERMAT-Vermutung für alle $n \geq 6$ folgen, und für $n = 3, 4, 5$ ist der Satz schon lange bekannt: Für $n = 4$ und möglicherweise auch $n = 3$ hatte FERMAT selbst bereits spätestens um 1640 einen (grob skizzierten) Beweis; den für $n = 4$ arbeitete BERNARD FRÉNICLE DE BESSY aus und veröffentlichte ihn 1676. EULER fand 1753 einen Beweis für den Fall $n = 3$, den er 1770 veröffentlichte. Er arbeitete dazu mit den dritten Einheitswurzeln. Ebenfalls mit Einheitswurzeln bewies ERNST EDUARD KUMMER die FERMAT-Vermutung für alle Exponenten, die durch eine sogenannte reguläre Primzahl teilbar sind, d.h. durch eine Primzahl, für die es im Ring der ganzen Zahlen im Körper $\mathbb{Q}(\zeta_p)$ eine eindeutige Primzerlegung gibt. (Eine Zahl aus einen Körper $K/\mathbb{Q}$ heißt ganz, wenn sie Nullstelle eines *normierten* Polynoms mit ganzzahligen Koeffizienten ist. Im Gegensatz zur Definition einer algebraischen Zahl wird hier also noch verlangt, daß der führende Koeffizient des Polynoms eins ist.) Zu diesen regulären Primzahlen gehört insbesondere auch die Zahl fünf.

Der derzeitige Stand der abc-Vermutung ist innerhalb der Mathematik umstritten. 2012 kündigte SHINICHI MOCHIZUKI vom Research Institute for Mathematical Sciences (RIMS) der Universität Kyoto einen Beweis an, der nach langer kontroverser Diskussion im Februar 2020 von den *Publications of the RIMS* zur Veröffentlichung angenommen wurde. Da MOCHIZUKI in seiner rund sechshundert Seiten langen Arbeit mit vielen, von ihm selbst entwickelten neuen und unkonventionellen Methoden arbeitet, wird der Beweis allerdings zumindest außerhalb Japans von den meisten Experten nicht akzeptiert.

Für weitere Informationen zu §2 und §3 sei auf einen Vortrag verwiesen, den SERGE LANG (1927 – 2005) im Jahr 1992 an der ETH 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.

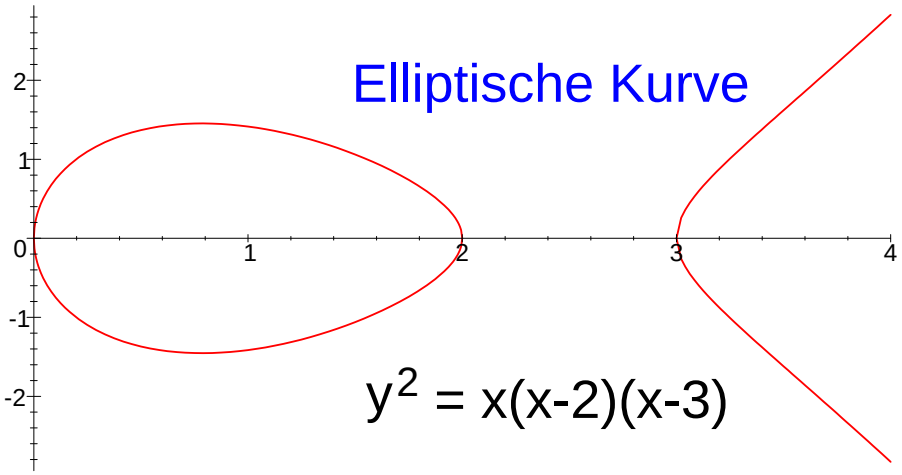
§4: Die Frey-Kurve

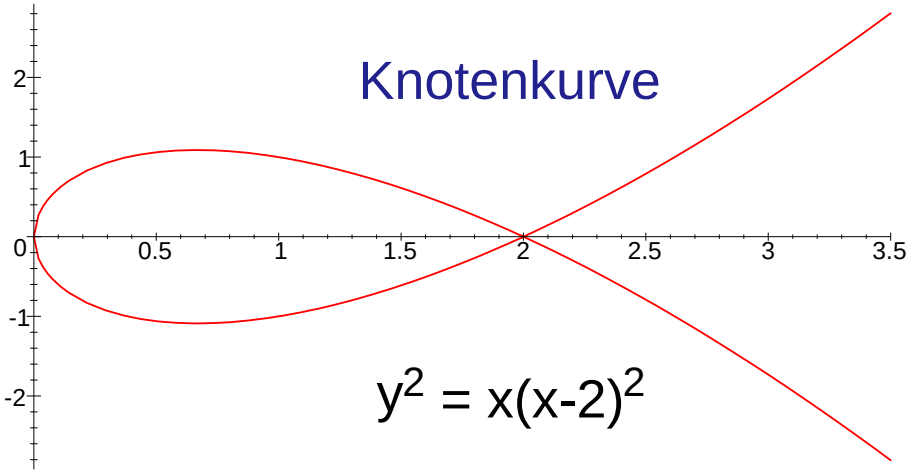
Da die FERMAT-Vermutung seit 1994 bewiesen ist, die abc-Vermutung aber immer noch offen, mußte der Beweis der FERMAT-Vermutung natürlich andere Wege gehen. Die meisten dieser Wege führen in Gebiete, die weit jenseits dessen liegen, was selbst ein guter auf Zahlentheorie spezialisierter Mathematiker im Laufe seines Studiums lernen kann. 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.

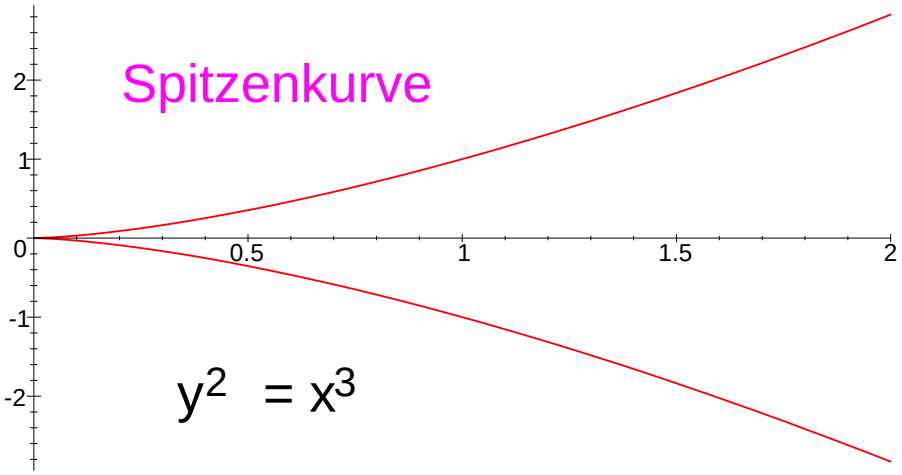
Der Anstoß kam 1984 von GERHARD FREY, damals Professor an der Universität Saarbrücken, wo er auf dem Gebiet der Arithmetik elliptischer Kurven arbeitete. (Von 1990 bis zu seiner Pensionierung im Jahr 2009 leitete er die Arbeitsgruppe Zahlentheorie am Institut für experimentelle Mathematik der (inzwischen mit Duisburg vereinigten) Universität Essen und beschäftigte sich unter anderem mit der Anwendung elliptischer 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;


Elliptische Kurve
2
1
0
-1
-2
1
2
3
4
$y^2 = x(x-2)(x-3)$


Knotenkurve
2
1
0
-1
-2
0.5
1
1.5
2
2.5
3
3.5
$y^2 = x(x-2)^2$


Spitzenkurve
2
1
0
-1
-2
0.5
1
1.5
2
$y^2 = x^3$

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 bereits FERMAT selbst gelöst, den Fall $n = 3$ wenig 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

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

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 betrachtete FREY die elliptische Kurve

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

die er aber nicht nur über den reellen oder komplexen Zahlen betrachtet, sondern auch über den Körpern $\mathbb{F}_p$.

FREYs Gleichung definiert genau dann eine elliptische Kurve, wenn alle drei Nullstellen verschieden sind, wenn also

$$a^\ell b^\ell (a^\ell + b^\ell) = a^\ell b^\ell c^\ell = (abc)^\ell$$

nicht verschwindet. Über $\mathbb{F}_p$ sind die drei Nullstellen genau dann verschieden, wenn p kein Teiler dieser Zahl ist, wenn p also keine der drei Zahlen a, b, c teilt.

Da $(abc)^\ell$ verglichen mit a, b, c ziemlich groß ist, heißt das, daß es im Verhältnis zur Größe der Koeffizienten 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 es für eine primitive p-te Einheitswurzel so etwas wie eine eindeutige Primzerlegung für die hier nicht definierten gazen Elemente von $\mathbb{Q}(\zeta)$ gibt). 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 mathematische Forschung erheblich wichtiger ist als die FERMAT-Vermutung) bewies WILES 1994.