IN WELCHE SCHUBLADE GEHÖRT DAS?

DUCO VAN STRATEN

Vortrag auf dem Mainzer-Mathe-Tag am 30. Mai 2018.

§1. *Die Poesie des Unendlichen*

Der indische Mathematiker und autodidaktische Formelvirtuose Ramanujan wurde von Hardy im Jahre 1914 nach Cambridge geholt, und der Kulturschock muss groß gewesen sein.

G. Hardy (1877-1947)

S. Ramanujan (1887-1920

In dem biographischen Kinofilm *The man who knew infinity* über Ramanujan mit Dev Patel in der Hauptrolle und Hardy gespielt von Jeremy Irons, kommt eine Szene im Hörsaal vor. Der Dozent (nicht Hardy) schreibt ein Integral an die Tafel, alle Studenten schreiben fleißig mit, nur Ramanujan sitzt da und schaut gebannt auf die Tafel. Der Dozent ist irritiert einen Inder in seiner Vorlesung zu haben und holt Ramanujan an die Tafel: Soll er doch zeigen, dass er es besser kann. Ramanujan schreibt das Ergebnis ohne zu zögern einfach hin: [1]

$$\int_0^1 \frac{dx}{\sqrt{x(1-x)(1-tx)}} = \pi\left(1+\left(\frac{1}{2}\right)^2 t+\left(\frac{1\cdot 3}{2\cdot 4}\right)^2 t^2+\left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)^2 t^3+\dots\right)$$

Der Dozent fragt: *How do you know?*, aber Ramanujan kann nur antworten *I don't know, I just do....* Nach der Vorlesung sagt der aufgebrachte Dozent zu Ramanujan: *You don't pull a stunt like that in my class! You don't belong here and you can tell your master, Hardy, I said as much as NOW GET OUT!*

§2. Was für Mathematik ist das eigentlich?

Ein Integral wird in eine schöne Potenzreihe entwickelt. Na und? Was ist das eigentlich für eine Sorte von Mathematik?

[1] Im Film kommt ein etwas anderes, aber eng verwandtes Integral vor.

Na ja, das ist klar, sagt der *Analytiker*, es geht um Integrale und unendliche Reihen, also Analysis, ganz eindeutig. Wenn du es genau wissen willst: Es ist ein vollständiges elliptisches Integral der ersten Sorte und erfüllt die Legendre Differentialgleichung:

$$\left(\theta^2 - t(\theta + \frac{1}{2})^2\right)\Phi(t) = 0, \quad \theta = t\frac{d}{dt}.$$

Es gibt viele Wandelformen dieses Integrals: Durch Substitution $x \mapsto tx$ transformiert sich das Integral zum Beispiel in die Form

$$\int_0^t \frac{dx}{\sqrt{x(x-1)(x-t)}}.$$

Papperlapapp, sagt der *Numeriker* und meint noch: die Reihe konvergiert nur für $|t| < 1$ und eignet sich eigentlich schlecht für die numerische Berechnung des Integrals. Da gibt es viel bessere Methoden. Speziell für solche elliptischen Integrale gibt es quadratisch konvergente Verfahren. Numerisch gesehen ist die Sache trivial.

Hoho, ruft der *Algebraiker*, es ist eigentlich Algebra: Die ganze Sache wird durch ein einziges Polynom bestimmt.

$$f(x,y) := y^2 - x(x-1)(x-t) \in K[x,y,t]$$

Für K können wir einen beliebigen Körper nehmen. Das Manipulieren solcher Integrale ist reine Algebra. Und wenn Du es genau wissen willst: unter dem Integralzeichen steht genau das *Residuum* einer rationalen Differentialform:

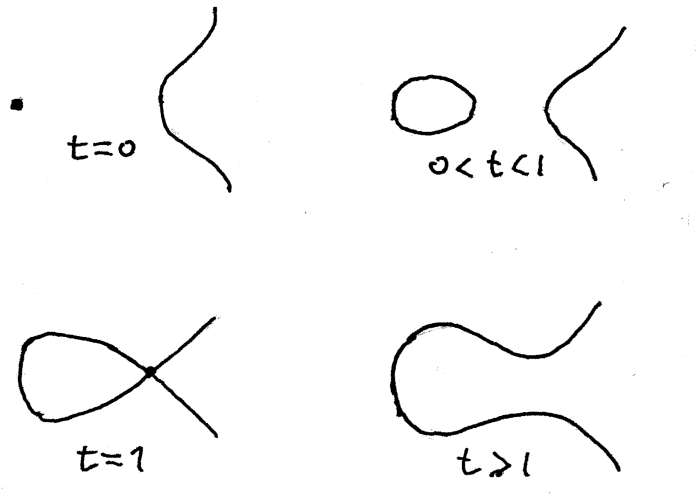
$$\omega_t = Res\left(\frac{dx \wedge dy}{f(x,y)}\right) = \frac{dx}{2y} = \frac{dx}{2\sqrt{x(1-x)(t-x)}}$$

Die Theorie der Normalformen für elliptische Integrale ist ein Kapitel der Algebra. Schau mal in Webers *Lehrbuch der Algebra*, da kann man wirklich mal was lernen.

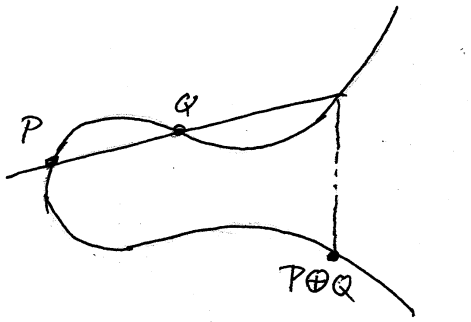
Unsinn, sagt der *Geometer*, es geht hier ganz klar um die Geometrie einer Kurve

$$E_t := \{(x,y) | f(x,y) = 0\},$$

wobei wir t als einen Parameter auffassen müssen. Und natürlich nehmen wir $K = \mathbb{R}$, dann können wir folgende Bilder zeichnen:

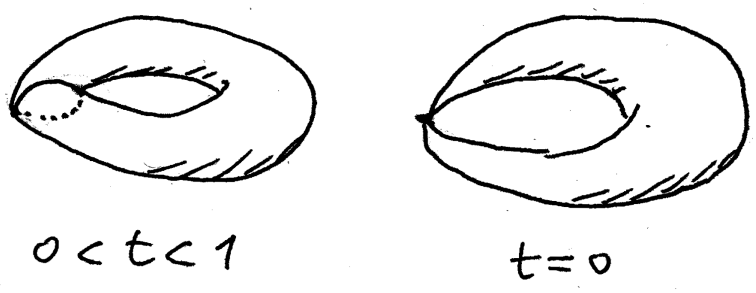


Solche Kurven werden *elliptische Kurven* genannt, obwohl sie mit Ellipsen bitter wenig zu tun haben. Übrigens, wenn wir einen Punkt ∞ zu E_t hinzufügen, können wir die Punkte von E_t durch ein hübsches geometrisches Verfahren addieren,



und als eine abelsche Gruppe auffassen (was dann aber wieder Algebra wäre...).

Jetzt mal ganz ruhig, sagt der *Topologe*, wenn wir nur $K = \mathbb{R}$ nehmen, sehen wir den größten Teil der Wahrheit nicht. Wir nehmen $K = \mathbb{C}$. Deine Kurve ist in Wirklichkeit ein Torus!



Für $t = 0$ wird eine Schleife auf dem Torus zusammen geschnürt, und es entsteht eine Art Wurst, das ist die singuläre Kurve. Und wenn Du es genau wissen willst: Das Integral lässt sich auch homologisch deuten: $\gamma_t \in H_1(E_t, \mathbb{Z})$ ist 1-Zyklus aus E_t und

$$[\omega_t] \in H^1_{dR}(E_t).$$

Wir haben es also mit einem *Periodenintegral*

$$\phi(t) = \int_{\gamma_t} \omega_t$$

zu tun. Da für $t = 0$ der Zyklus γ_t zu einem Punkt wird, nennen wir diese dem *verschwindenden Zykel*.

Alles schön und gut, sagt der *Zahlentheoretiker*, aber die Reihe hat in Wirklichkeit mit der Zählung von Punkten auf der Kurve E_t zu tun. Wenn Du es genau wissen willst: Nimm eine Primzahl und $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, den Körper mit p Elementen. Wir betrachten

$$E_t(\mathbb{F}_p) := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid \ y^2 = x(x-1)(x-t)\}$$

Es ist nicht schwer, folgenden Satz zu zeigen:

Satz

Schreibe

$$H_p(t) := 1 + \left(\frac{1}{2}\right)^2 t + \left(\frac{1 \cdot 3}{2 \cdot 4}\right) t^2 + \ldots + (...)t^{p-1} = \sum_{k=0}^{p-1} \binom{-1/2}{k}^2 t^k$$

für die nach p Gliedern abgebrochene Reihe. Dann gilt:

$$\#E_t(\mathbb{F}_p) = -(-1)^{\frac{p-1}{2}} H_p(t) \mod p$$

Als Beispiel, nimm $p = 11$ und $t = 3$. Wenn x den Körper $\mathbb{F}_p$ durchläuft, dann erhalten wir folgende Lösungen $(x, y) \in E_3(\mathbb{F}_{11})$:

x	0	1	2	3	4	5	6	7	8	9	10
$x(x-1)(x-3)$	0	0	9	0	1	7	2	3	5	3	3
y	0	0	3, 8	0	1, 10	–	–	5, 6	4, 7	5, 6	5, 6

Wir stellen also fest, dass die Kurve $E_3(\mathbb{F}_{11})$ 15 Punkte besitzt:

$$\#E_3(\mathbb{F}_{11}) = 3 + 2 \cdot 6 = 15.$$

Und in der Tat ist:

$$H_{11}(3) = \frac{200852972940865}{68719476736} \equiv 4 \mod 11 = 15 \mod 11!$$

§3. *Algebraische Geometrie*

Natürlich haben alle Kollegen aus der obenstehenden Geschichte irgendwie recht: in der Mathematik hängt eben Alles mit Allem zusammen. Die *Algebraische Geometrie* nun ist auch der verzweifelte Versuch, alle diese verschiedenen Gesichtspunkte zu vereinen und ihre Beziehung klar darzulegen.
Der Zusammenhang zwischen Periodenintegralen und Anzahlen von Punkte $\mod p$ geht vielleicht auf Gauss und viel später Igusa zurück und deutet auf eine tieferliegende Beziehung zwischen Topologie, Analysis und Arithmetik hin. Ein konzeptueller Beweis in größerer Allgemeinheit wurde von Manin [5] gegeben und eine schöne elementare Darstellung findet man in dem Buch von Clemens [4].

Nach der Philosophie von Weil bestimmt die Wirkung des *Frobenius Morphismus* (induziert von der Abbildung $x \mapsto x^p$) auf den Kohomologie-Gruppen von Varietäten über Körpern der Charakteristik p die Anzahl ihrer Punkte. Ist zum Beispiel C eine glatte projektive Kurve über $\mathbb{F}_p$, so gilt

$$\#C(\mathbb{F}_p) = 1 - a_p + p$$

wobei

$$a_p = Spur\left(F : H^1(C) \to H^1(C)\right),$$

die Spur von F auf der ersten étalen Kohomologie ist. Es ist

$$a_p \mod p = Spur\left(F : H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)\right)$$

was ausreicht, wenn wir nur an der Zahl der Punkte $\mod p$ interessiert sind.

In unserer Situation hängt E auch noch von einem Parameter t ab, $E = E_t$, also ist auch $a_p = a_p(t)$. Man kann zeigen, dass $a_p(t) \mod p$ genau wie $H_p(t)$ Lösung der Kongruenz Differentialgleichung

$$(\theta^2 - t(\theta + \frac{1}{2})^2)\Psi(t) = 0 \mod p$$

ist und tatsächlich gilt:

$$a_p(t) = (-1)^{\frac{p-1}{2}} H_p(t) \mod p$$

Die hier skizzierte Geschichte bezieht sich auf den Fall einer *elliptischen Kurve* E_t. In der algebraischen Geometrie werden auch Verallgemeinerungen dieses Falls auf spezielle Varietäten höherer Dimension untersucht, wie K3-Flächen, Hyperkähler Mannigfaltigkeiten und Calabi-Yau Mannigfaltigkeiten. Das sind Forschungsthemen, welche im Sonderforschungsbereich Transregio 45 (Mainz, Bonn und Essen) eine große Rolle spielen.

§4. Nachtrag

Am einfachsten erhält man die Reihenentwicklung, indem man im Integral

$$\Phi(t) := \int_0^1 \frac{dx}{\sqrt{x(1-x)(1-tx)}}$$

den Integrand in eine Reihe nach t entwickelt und dann termweise integriert:

$$\frac{1}{\sqrt{1-tx}} = \sum_{k=0}^{\infty} \binom{-1/2}{k} t^k x^k,$$

$$\Phi(t) := \sum_{n=0}^{\infty} \int_0^1 \frac{x^n dx}{\sqrt{x(1-x)}} \binom{-1/2}{n} t^n$$

Da aber nach der Wallisschen Formel auch gilt

$$\int_0^1 \frac{x^n dx}{\sqrt{x(1-x)}} = \binom{-1/2}{n},$$

erhalten wir

$$\Phi(t) = \sum_{n=0}^{\infty} \binom{-\frac{1}{2}}{n}^2 t^n$$

Bemerkenswert ist noch

$$\binom{-\frac{1}{2}}{n}^2 = \frac{1}{4^{2n}} \binom{2n}{n}^2,$$

so dass wir es im Wesentlichen mit den Quadraten der zentralen Binomialkoeffizienten $\binom{2n}{n}$ zu tun haben. Da freuen sich auch die *Kombinatoriker* und *Stochastiker*! Betrachten wir Wege im Standard quadratischen Gitter $\mathbb{Z}^2$ der Länge $2n$, die bei $(0,0)$ anfangen und enden, so ist deren Anzahl

$$a_n = \binom{2n}{n}^2.$$

Dies sieht man am einfachsten, wenn man bedenkt, daß die Anzahl solcher Wege genau der konstante Term der Laurentreihe

$$(x + \frac{1}{x} + y + \frac{1}{y})^{2n}$$

ist. Also ist die *Wahrscheinlichkeit*, nach einer Gitter-Irrfahrt in genau $2n$ Schritten wieder zu Hause zu sein, gerade der Koeffizient von t^n in unsere Reihe:

$$\binom{-1/2}{n}^2 = \frac{1}{4^{2n}}\binom{2n}{n}^2!$$

Im Film kommt das vollständige elliptische Integral der ersten Sorte in *Legendre Normalform*

$$K(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

vor, was eine geringfügig andere Entwicklung

$$K(k) = \frac{\pi}{2}\left(1 + \left(\frac{1}{2}\right)^2 k^2 + \left(\frac{1\cdot 3}{2\cdot 4}\right)^2 k^4 + \left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)^2 k^6 + \dots\right)$$

besitzt. Ramanujan hatte Recht, rechnen Sie es nach!

§5. Beweis des Satzes

Es sei p eine ungerade Primzahl, $f(x) \in \mathbb{F}_p[x]$ ein Polynom. Betrachte die Menge

$$C := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid \quad y^2 = f(x)\}.$$

Aufgabe 1: Benutze die Tatsache, daß die multiplikative Gruppe $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ von $\mathbb{F}_p$ zyklisch ist, um zu zeigen:

$$a \in \mathbb{F}_p \quad \text{ist ein Quadrat, genau dann wenn } \; a^{\frac{p-1}{2}} = 1.$$

Aufgabe 2: Folgere hieraus:

$$\#C = \sum_{x\in\mathbb{F}_p}(1 + f(x)^{\frac{p-1}{2}}) \equiv \sum_{x\in\mathbb{F}_p} f(x)^{\frac{p-1}{2}} \mod p.$$

Aufgabe 3: Zeige, daß für $a \in \mathbb{F}_p^*$ und $k \in \mathbb{N}$ gilt:

$$\sum_{x\in\mathbb{F}_p} x^k = a^k \sum_{x\in\mathbb{F}_p} x^k$$

Folgere, daß

$$\sum_{x\in\mathbb{F}_p} x^k = \begin{cases} 0 & \text{wenn} \quad (p-1) \nmid k \\ -1 & \text{wenn} \quad (p-1) \mid k \end{cases}$$

Aufgabe 4: Folgere aus 2) und 3), daß wenn $Grad(f) \leq 3$:

$$\#C \equiv -[f(x)^{\frac{p-1}{2}}]_{p-1} \mod p$$

wobei

$$[...]_n := \text{Koeffizient von } \; x^n \; \text{ in ....}$$

Aufgabe 5: Für $f(x) = x(x-1)(x-t)$ ist also

$$\#C \equiv -[(x-1)(x-t)^{\frac{p-1}{2}}]_{\frac{p-1}{2}} \mod p.$$

Benutze jetzt die binomische Formel, um zu zeigen:

$$\#C \equiv -(-1)^{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k}^2 t^k$$

Aufgabe 6: Zeige

$$\binom{\frac{p-1}{2}}{k} = \frac{1}{k!} \cdot \frac{p-1}{2} \cdot \frac{p-3}{2} \cdots \frac{p-(2k-1)}{2} \equiv \frac{1}{k!} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdots \frac{-(2k-1)}{2} \equiv= \binom{\frac{-1}{2}}{k}$$

Aufgabe 7: Folgere den Satz aus dem Vortrag. Bemerke, daß man in der Reihe die Summe nur bis $\frac{p-1}{2}$ laufen lassen muss, da

$$\binom{\frac{-1}{2}}{k} \equiv 0 \mod p,$$

für $\frac{p-1}{2} < k \leq p-1$.

References

[1] *The Man who knew Infinity* (deutsch: *Die Poesie des Unendlichen*), Film von Matthew Brown aus (2015), nach Vorlage der gleichnämige Biographie von Kanigel.

[2] G. Hardy, *Ramanujan. Twelve Lectures on Subjects suggested by his Life and Work.*, Cambridge (1940).

[3] R. Kanigel, *The Man Who Knew Infinity: a Life of the Genius Ramanujan*, New York: Charles Scribner's Sons (1991).

[4] H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum Press, New York, (1980).

[5] Y. Manin, *The HasseWitt matrix of an algebraic curve*, Transl., Ser. 2, Am. Math. Soc. 45: 245 - 246.

[6] H. Weber, *Lehrbuch der Algebra*, (Band I,II,III), Vieweg und Sohn, (1898-1908)