

Von den Fermatschen Zahlen

RALPH STREBEL

Unter den Fermatschen Zahlen versteht man die Folge der Zahlen

$$F_m = 2^{(2^m)} + 1. \quad (1)$$

Ihre ersten 5 Glieder berechnen sich zu $2^1 + 1 = 3$, $2^2 + 1 = 5$, dann $2^4 + 1 = 17$, $2^8 + 1 = 257$ und $2^{16} + 1 = 65\,537$. Diese Zahlen sind alle prim; Fermat usserte 1640 die Vermutung, jede der Zahlen F_m sei eine Primzahl.

In diesem Aufsatz will ich erklären, wie Fermat zu den nach ihm benannten Zahlen kam, wie Euler herausfand, dass F_5 keine Primzahl ist, und wie Gauss zeigen konnte, dass sich jedes regelmässige Vieleck, dessen Eckenzahl eine Fermatsche Primzahl ist, mit Zirkel und Lineal konstruieren lässt.

Von den vollkommenen zu den Fermatschen Zahlen

Euklid nennt eine natürliche Zahl $n > 1$ *vollkommen*, wenn sie mit der Summe ihrer *echten* Teiler bereinstimmt (Elemente, VII, Def. 22); dabei gilt 1 als echter Teiler von n , nicht aber n . Beispiele sind $6 = 1 + 2 + 3$ und $28 = 1 + 2 + 4 + 7 + 14$. Im letzten Resultat des Buches IX beschreibt Euklid dann ein Verfahren, das es erlaubt, weitere vollkommene Zahlen zu gewinnen:

Satz 1 (Elemente, IX, 36). *Verschafft man sich beliebig viele Zahlen, von der Einheit aus in Reihe nach dem Verhältnis $1 : 2$, bis die Summe aus allem eine Primzahl wird, und bildet die Summe, mit dem letzten Glied vervielfacht, die Zahl A_q , so muss A_q vollkommen sein.*

Der Beweis ist einfach. Sei $q > 1$ die Anzahl der Glieder der geometrischen Progression und

$$A_q = (1 + 2 + 4 + \dots + 2^{q-1}) \cdot 2^{q-1} = (2^q - 1)2^{q-1} = 2^{q-1} \cdot M_q;$$

dabei habe ich $M_q = 2^q - 1$ gesetzt. Offensichtlich besitzt A_q die echten Teiler $1, 2, 4, \dots, 2^{q-1}$ und $M_q, 2 \cdot M_q, \dots, 2^{q-2} \cdot M_q$; die Summe dieser Teiler beträgt

$$(1 + \dots + 2^{q-1}) + (1 + \dots + 2^{q-2}) \cdot M_q = M_q + (2^{q-1} - 1) \cdot M_q = 2^{q-1} \cdot M_q = A_q.$$

Daher ist A_q genau dann vollkommen, wenn A_q keine weiteren echten Teiler hat. Aus der Eindeutigkeit der Primfaktorzerlegung folgt andererseits, dass A_q genau dann keine weiteren Teiler besitzt, wenn M_q eine Primzahl ist.

Euler fand 1747 eine Umkehrung von Satz 1 ([6, pp. 354–355]); er bewies, dass jede *gerade* vollkommene Zahl die von Euklid angegebene Form hat. Ob es *ungerade* vollkommene Zahlen gibt, ist eine auch heute noch ungelöste Frage.

Frenicle de Bessy fragt Fermat nach einer grossen vollkommenen Zahl

Der Name *vollkommene* Zahl deutet darauf hin, dass diese Zahlen Mathematiker, aber auch Zahlenliebhaber, seit alters her fasziniert haben. Im 17. Jahrhundert beschäftigten sich unteren anderen M. MERSENNE (1588–1648), B. FRENICLE DE BESSY (um 1605–1675) und P. FERMAT (1601(?)–1665) mit diesen Zahlen. Im Jahre 1640 fragte Frenicle Fermat, ob es eine vollkommene Zahl zwischen 10^{20} und 10^{22} gebe; dabei dachte er an die mit Satz 1 konstruierten Zahlen. Eine kurze Rechnung zeigt, dass eine vollkommene Zahl genau dann im gewünschten Intervall liegt, wenn eine der Zahlen M_q mit $q \in \{34, 35, 36, 37\}$ eine Primzahl ist. Nun wusste Fermat, dass M_q höchstens dann prim ist, wenn der Exponent q eine Primzahl ist: jeder von 1 verschiedene

Teiler q_1 von q gibt nmlich Anlass zum Teiler M_{q_1} von M_q . Also war der Kern des Problems von Frenicle die Frage, ob die Zahl

$$M_{37} = 2^{37} - 1 = 137\,438\,953\,471$$

prim ist. Ist sie keine Primzahl, hat sie einen Primteiler unterhalb von $\sqrt{M_{37}} \approx 370\,727.6$; da es aber ber 30 000 solche Primzahlen gibt, wird man nicht erwarten, dass Fermat versuchte, die Antwort mit der naiven Methode zu finden. Vielmehr zog er einen nach ihm benannten Satz heran:

Satz 2. *Fr jede Primzahl p und jede natrliche Zahl a , die kein Vielfaches von p ist, gelten die folgenden Aussagen:*

(i) *Die Zahl $a^{p-1} - 1$ ist durch p teilbar; es gilt also $a^{p-1} \equiv 1 \pmod{p}$.*

(ii) *Sei n_0 die kleinste positive Lsung der Kongruenz $a^n \equiv 1 \pmod{p}$. Dann teilt n_0 jede Lsung n dieser Kongruenz; insbesondere teilt n_0 die Zahl $p - 1$.*

Fermat konnte mit Satz 2 wie folgt weiterschliessen. Ist p ein Primteiler von M_{37} , so gelten die Kongruenzen $2^{37} - 1 \equiv 0$, also auch $2^{37} \equiv 1$ modulo p . Da 37 eine Primzahl ist, folgt aus Satz 2 (ii), dass 37 die kleinste der positiven Lsungen der Kongruenz $2^n \equiv 1 \pmod{p}$ ist und dass p die Form $37 \cdot k + 1$ hat; da p die ungerade Zahl M_{37} teilt, muss der Parameter k gerade sein. Die Zahl $74 + 1 = 75$ ist keine Primzahl, hingegen haben $2 \cdot 74 + 1 = 149$ und $3 \cdot 74 + 1 = 223$ diese Eigenschaft. Und 223 teilt M_{37} .

Der Quotient $M_{37}/223$ ist gleich 616 318 177; er ist eine Primzahl. Ob Fermat dies nachgeprft hat, ist nicht bekannt.

Fermatsche Zahlen

Die Zahlen M_q haben die Form $a^n - 1$; interessiert man sich nicht nur fr die Frage, ob $a^n - 1$ eine Primzahl ist, sondern allgemeiner fr die Primfaktorzerlegung dieser Zahlen, so wird man fr $n = 2m$ auf die Zerlegung von Zahlen der Form $a^m + 1$ gefhrt. Falls m einen *ungeraden* Primteiler p hat, etwa $m = m_1 \cdot p$, kann $a^m + 1$ zerlegt werden, denn $a^m + 1 = (a^{m_1} + 1) \cdot ((a^{m_1})^{p-1} - \dots - a^{m_1} + 1)$. Nur dann also kann $a^m + 1$ eine Primzahl sein, wenn m eine Potenz von 2 ist. Fr $a = 2$ ergeben sich so die Fermatschen Zahlen $F_m = 2^{(2^m)} + 1$.

In einem Brief an Frenicle, ebenfalls aus dem Jahre 1640, notierte Fermat die Werte der Zahlen F_m fr $m \leq 6$, insbesondere

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 \quad \text{und} \quad F_6 = 2^{64} + 1 = 18\,446\,744\,073\,709\,551\,617. \quad (2)$$

Er sprach die Vermutung aus, die Zahlen F_m seien alle Primzahlen; er wiederholte sie spter, zum Beispiel in Briefen vom August 1659 an P. de CARCAVI (um 1600–1684) und an C. HUYGENS (1629–1695).

Euler und die Fermatschen Zahlen

Die zahlentheoretischen Untersuchungen Fermats gerieten nach seinem Tode in Vergessenheit. Dies hatte mehrere Grnde: zum einen interessierte die Zahlentheorie bloss wenige Mathematiker des 17. Jahrhunderts; dann teilte Fermat seine Ergebnisse nur in Briefen an Mathematiker eines kleinen Kreises mit oder vertraute sie den Rndern seines Exemplars der Werke von DIOPHANT (3. Jahrhundert n. Chr.) an. Auch schrieb er fast keinen seiner Beweise in ausfhrlicher Form auf.

Als daher Leonhard EULER (1707–1783) im Jahre 1730 anfang, sich der Zahlentheorie zuzuwenden, angeregt durch Briefe von C. GOLDBACH (1690–1764), kannte er die Ergebnisse Fermats nur ungenau; auch glaubte er, Fermat habe seine Resultate nur *induktiv*, d. h. durch Zahlenbeispiele, begrndet. Ein erster, wichtiger Schritt bestand fr Euler daher darin, Beweise fr die Fermatschen Behauptungen zu suchen.

Euler findet einen Teiler von F_5

In der Arbeit [3] beschftigt sich Euler mit den Fermatschen Zahlen; es ist seine erste Arbeit ber Zahlentheorie. Euler betont, diese Zahlen wrden, sofern sie denn prim sind, eine konkrete, sehr schnell wachsende Folge von

Primzahlen abgeben, was nützlich wäre. Aus einem Grund, den er nicht durchschaute, sei aber bereits F_5 keine Primzahl mehr, sie sei nämlich durch 641 teilbar.

Wie Euler den Teiler 641 entdeckte, teilt er in einer späteren Arbeit mit (siehe [4]). Ist, so die Überlegung Eulers, p ein Primteiler von F_5 , so gilt $2^{32} + 1 \equiv 0 \pmod{p}$, also auch $2^{32} \equiv -1 \pmod{p}$ und $2^{64} \equiv 1 \pmod{p}$. Nach Satz 2 teilt die kleinste positive Zahl n_0 , welche die Kongruenz $2^n \equiv 1 \pmod{p}$ erfüllt, den Exponenten 64; insbesondere ist n_0 eine Zweierpotenz. Aus $2^{32} \equiv -1 \pmod{p}$ folgt dann, dass $n_0 = 64$ sein muss, weshalb p die Form $1 + 64 \cdot k$ aufweist. Von den 10 Zahlen

$$64 + 1 = 65, \quad 64 \cdot 2 + 1 = 129, \quad 193, \quad 257, \dots, 449, \quad 513, \quad 577 \text{ und } 641$$

sind die dritte, vierte, siebte, neunte und zehnte prim. Die zehnte teilt F_5 .

Beweis des kleinen Satzes von Fermat

In [3] spricht Euler den (kleinen) Satz von Fermat, also Satz 2, aus und leitet daraus verschiedene Folgerungen her; er begründet diese Resultate aber nicht. In der Arbeit [4], die etwa im Jahre 1736 verfasst worden, gibt er dann zwei Beweise für Satz 2. Der zweite Beweis geht von der Identität

$$(a + 1)^p = a^p + \binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a + 1$$

aus; dabei bezeichnen p eine Primzahl und a eine beliebige ganze Zahl. Da die ausgeschriebenen Binomialkoeffizienten alle Vielfache von p sind, vereinfacht sich die Identität modulo p zu $(a + 1)^p \equiv a^p + 1$. Setzt man nun a der Reihe gleich $1, 2, \dots$, erhält man schrittweise die Beziehungen

$$2^p \equiv 1^p + 1 = 2, \quad 3^p \equiv 2^p + 1 \equiv 2 + 1 = 3, \dots, (a + 1)^p \equiv a^p + 1 \equiv a + 1, \dots$$

Sie zeigen, dass die Kongruenz $a^p \equiv a \pmod{p}$ für jede natürliche Zahl richtig ist. Falls a kein Vielfaches von p ist, so induziert die Multiplikation mit a eine Bijektion μ_a der Menge \mathbb{F}_p der Äquivalenzklassen von \mathbb{Z} modulo p . Aus $a^p \equiv a \pmod{p}$ folgt daher die Kongruenz $a^{p-1} \equiv 1 \pmod{p}$. Sie beweist Teil (i) von Satz 2.

Nun sei n_0 der kleinste der positiven Exponenten n , für welche die Kongruenz $a^n \equiv 1 \pmod{p}$ richtig ist. Sei n_1 ein Exponent mit $a^{n_1} \equiv 1 \pmod{p}$ und sei r der Rest der Division von n_1 durch n_0 , etwa $n_1 = n_0 \cdot s + r$. Aus der Kongruenz

$$1 \equiv a^{n_1} = (a^{n_0})^s \cdot a^r \equiv 1 \cdot a^r \pmod{p}$$

sieht man, dass der Rest r gleich 0 sein muss. Dieses Argument rechtfertigt Teil (ii) von Satz 2.

In [5] gibt Euler einen ganz anderen Beweis. Seien p eine Primzahl und b eine ganze Zahl, die von p nicht geteilt wird. Dann induziert die Multiplikation mit b eine bijektive Abbildung von \mathbb{F}_p auf sich; insbesondere gibt es eine Restklasse \bar{b}' mit $\bar{b} \cdot \bar{b}' = \bar{1}$.¹ Nun sei $\bar{a} \in \mathbb{F}_p$ eine von $\bar{0}$ verschiedene Restklasse. Da \mathbb{F}_p endlich ist, müssen zwei Glieder der geometrischen Reihe $\bar{1}, \bar{a}, \bar{a}^2, \bar{a}^3, \dots$, etwa \bar{a}^{n_1} und \bar{a}^{n_2} mit $n_1 < n_2$, gleich sein; da μ_a bijektiv ist, ist dann $\bar{a}^{n_2 - n_1} = \bar{1}$. Sei n_0 die kleinste der positiven Zahlen mit $\bar{a}^{n_0} = \bar{1}$.² Dann sind die Glieder der Folge $\bar{1}, \bar{a}, \dots, \bar{a}^{n_0 - 1}$ paarweise verschieden. Falls diese Folge alle Elemente von $\mathbb{F}_p \setminus \{0\}$ enthält, ist $n_0 = p - 1$ und Satz 2 ist bewiesen. Andernfalles gibt es eine Restklasse $\bar{b}_1 \in \mathbb{F}_p \setminus \{0\}$, die in der Folge der Potenzen von \bar{a} nicht vorkommt. Da μ_{b_1} bijektiv ist, sind die Glieder der Folge $\bar{b}_1 \cdot \bar{1}, \bar{b}_1 \cdot \bar{a}, \dots, \bar{b}_1 \cdot \bar{a}^{n_0 - 1}$ paarweise verschieden; ferner enthalten die beiden Folgen kein gemeinsames Element. Enthalten die Folgen zusammen alle Elemente von $\mathbb{F}_p \setminus \{0\}$, so ist $p - 1 = 2 \cdot n_0$ und Satz 2 ist bewiesen. Andernfalles konstruiert man nach dem gleichen Verfahren weitere Folgen, bis dass die endliche Menge $\mathbb{F}_p \setminus \{0\}$ mit disjunkten Teilmengen der Größe n_0 ausgeschöpft ist.³

Fermat konnte beide der obigen Beweismethoden gekannt haben, doch lässt sich diese Vermutung nicht mit Dokumenten belegen.

¹Ausgedrückt in der Sprache des 20. Jahrhunderts heißt dies, dass $\mathbb{F} \setminus \{\bar{0}\}$ bezüglich der Multiplikation eine Gruppe mit $p - 1$ Elementen ist.

²Es ist n_0 die Ordnung der von \bar{a} in $\mathbb{F}_p \setminus \{0\}$ erzeugten Untergruppe.

³Dies ist im wesentlichen das Argument, mit dem man heute nachweist, dass die Ordnung einer Untergruppe H einer endlichen Gruppe G die Ordnung von G teilt.

Teiler der Fermatschen Zahlen F_m mit $m > 5$

Satz 2 liefert für jede Fermatsche Zahl F_m eine Bedingung an die möglichen Primteiler von F_m . Wie zuvor sieht man ein, dass jeder Primteiler von F_m die Form $p = 2^{m+1} \cdot k_1 + 1$ haben muss; mit einem Zusatzargument kann man noch beweisen, dass k_1 gerade sein muss, der Primteiler also die Form $p = 2^{m+2} \cdot k + 1$ hat (siehe [10, p. 71]). Daraus folgt leicht, dass alle Teiler von F_m die Form $2^{m+2} \cdot k + 1$ haben müssen.

Betrachten wir nun noch einmal die Zahl F_5 . Jeder Teiler von F_5 liegt in der arithmetischen Progression $f: k \mapsto 2^{5+2} \cdot k + 1 = 128 \cdot k + 1$. Die Glieder f_1, f_2, f_3 und f_4 teilen F_5 nicht, wohl aber $f_5 = 641$. Nun ist es keineswegs so, dass jede zusammengesetzte Fermatsche Zahl F_m einen Primteiler $p = 2^{m+1} \cdot k + 1$ mit kleinem Parameter k aufweist. So sind sowohl F_6 als auch F_7 Produkte von zwei größeren Primzahlen; es gilt nämlich ([8, pp. 94–95]):

$$F_6 = 274\,177 \cdot 67\,280\,421\,310\,721 \text{ mit } 274\,171 = 2^8 \cdot 1071 + 1, \tag{3}$$

$$F_7 = p_{17} \cdot p_{22} \text{ mit } p_{17} = 59\,649\,589\,127\,497\,217 = 2^9 \cdot 116\,503\,103\,764\,643 + 1. \tag{4}$$

(Die Zahlen p_{17} und p_{22} bezeichnen Primzahlen mit 17, beziehungsweise 22, Dezimalziffern.) Geht man wie Euler vor, wird man die Teiler von F_6 und F_7 nicht finden.

Erstaunlich ist nun, dass weit größere Fermatsche Zahlen Primteiler haben, deren Parameter k klein sind; dies belegt die nächste Tabelle. In ihr sind alle Paare (m, k) mit $5 \leq m \leq 300$ und $1 \leq k \leq 100$ aufgeführt, die zu einem Primteiler $2^{m+2} \cdot k + 1$ von F_m gehören.

m	5	11	18	23	36	38	39	55	63	73	117	125	144	207	226	228
k	5	39	13	5	10	6	21	29	36	5	14	5	34	3	30	58

Man beachte, dass F_{23} bereits etwa $2^{23} \cdot \log_{10} 2 \approx 2.525 \cdot 10^6$ Dezimalziffern hat, also etwa die Größenordnung der größten Primzahlen, die heute explizit bekannt sind. Dass man Teiler von noch deutlich größeren Fermatschen Zahlen in wenigen Sekunden mit einem Tischrechner finden kann — ich habe sie mit einem Macintosh der Generation 4 aufgespart, hängt an dem Umstand, dass p genau dann F_m teilt, wenn die Kongruenz $2^{2^m} \equiv -1 \pmod{p}$ zutrifft. Modulo p läuft die Berechnung von $2^{(2^m)}$ aber auf ein m -faches Quadrieren von Zahlen kleiner als p und anschließende Division durch p hinaus. Die unermessliche Größe der Zahl F_{228} — sie hat etwa $2^{228} \cdot \log_{10} 2 \approx 1.3 \cdot 10^{68}$ Dezimalziffern — tritt in dieser Rechnung nie in Erscheinung.

Dies erklärt, warum man oberhalb von $m = 20$ zwar in gewissen Fällen Teiler von Fermatschen Zahlen finden kann, nicht aber mit einem bekannten, systematischen Test. Bei diesem berechnet man $3^{(F_m-1)/2}$ modulo F_m . Genau dann ist F_m eine Primzahl, wenn das Ergebnis kongruent -1 modulo F_m ist. Die Berechnung der Restklasse von $3^{(F_m-1)/2}$ modulo F_m benötigt nun aber ein $(2^m - 1)$ -faches Quadrieren und Dividieren von Zahlen, welche die Größenordnung von F_m haben können.

Gauss und die Fermatschen Primzahlen

Unsere bisherigen Ergebnisse über die Fermatschen Zahlen zeigen folgendes: die Folge $m \mapsto F_m$ wächst sehr schnell an und alle ihre Glieder unterhalb von 10^9 sind prim. Viele der noch größeren Glieder sind nachweislich zusammengesetzte Zahlen. C. F. GAUSS (1777–1855) entdeckte um 1800 eine neue Eigenschaft der Fermatschen Primzahlen. Diese neue Eigenschaft will ich im dritten Teil meines Aufsatzes zur Sprache bringen.

Sei p eine ungerade Primzahl. Die komplexen Nullstellen des Polynoms $X^p - 1$ sind die Zahlen $1, r_p = \exp(2\pi i/p), r_p^2, \dots, r_p^{p-1}$; sie bilden die Ecken eines regelmässigen p -Eckes, das dem Einheitskreis $\{z \in \mathbb{C} \mid z \cdot \bar{z} = 1\}$ eingeschrieben ist. Seit der Antike ist bekannt, dass das regelmässige p -Eck mit Zirkel und Lineal konstruiert werden kann. Algebraisch kann man dies so einsehen.

Die Zahl $r = r_5 = e^{2\pi i/5}$ ist Nullstelle des Polynoms $\Phi_5 = X^4 + X^3 + X^2 + X + 1$ und daher Nullstelle der rationalen Funktion

$$X^2 + X + 1 + X^{-1} + X^{-2} = (X + X^{-1})^2 + (X + X^{-1}) - 1.$$

Folglich ist $2 \cos(2\pi/5) = r + r^{-1}$ eine Nullstelle des Polynoms $Y^2 + Y - 1$ und daher gleich $\frac{1}{2}(\sqrt{5} - 1)$. Dieser Ausdruck für $2 \cos(2\pi/5)$ zeigt, dass die Ecke r mit Zirkel und Lineal konstruiert werden kann.

Das Polynom Y^2+Y-1 lässt sich mit einer anderen Methode finden. Dazu betrachtet man neben $2 \cos(2\pi/5) = r + r^{-1}$ noch $2 \cos(4\pi/5) = r^2 + r^{-2}$. Das quadratische Polynom mit Leitkoeffizient 1, das diese 2 Zahlen als Nullstellen hat, berechnet sich dann zu

$$\begin{aligned} (Y - (r + r^4)) \cdot (Y - (r^2 + r^3)) &= Y^2 - (r + r^2 + r^3 + r^4) \cdot Y + (r + r^4) \cdot (r^2 + r^3) \\ &= Y^2 + Y + (r^3 + r^4 + r^6 + r^7) = Y^2 + Y + (r^3 + r^4 + r + r^2), \end{aligned}$$

stimmt also mit dem zuvor gefundenen Polynom $Y^2 + Y - 1$ überein.

Konstruktion des regelmässigen Siebzehneckes

Die Zahl $5 = 2^2 + 1$ ist eine Fermatsche Primzahl. Gauss legte in seinem berühmten Buch des Titels *Disquisitiones arithmeticae* dar, wie die zweite der oben beschriebenen Methoden auf andere Fermatsche Primzahlen verallgemeinert werden kann. Im Falle der Primzahl $17 = 2^4 + 1$ geht er so vor.

Das Polynom $\Phi_{17} = X^{16} + X^{15} + \dots + X + 1$ hat die 16 Nullstellen

$$r = e^{2\pi i/17}, r^2, r^3, \dots, r^{16}.$$

Gauss unterteilt die Menge dieser Nullstellen in zwei Teilmengen $\mathcal{N}_{8,0}$ und $\mathcal{N}_{8,1}$ mit je 8 Elementen und zerlegt danach jede der Mengen $\mathcal{N}_{8,0}$ und $\mathcal{N}_{8,1}$ in zwei Teilmengen mit je 4 Elementen; seien $\mathcal{N}_{4,0}$ und $\mathcal{N}_{4,2}$, beziehungsweise $\mathcal{N}_{4,1}$ und $\mathcal{N}_{4,3}$ diese Teilmengen. Zum Schluss bildet er aus jeder der Vierermengen zwei Zweiermengen. Diesen Teilmengen nun ordnet Gauss Summen zu; er nennt sie *Perioden*. Die 8-gliedrigen Perioden sind $\eta_{8,0} = \sum\{r \mid r \in \mathcal{N}_{8,0}\}$ und $\eta_{8,1} = \sum\{r \mid r \in \mathcal{N}_{8,1}\}$; die vier 4-gliedrigen Perioden $\eta_{4,\ell}$ mit $\ell = 0, 1, 2, 3$ und die acht 2-gliedrigen Perioden $\eta_{2,\ell}$ werden analog definiert.

Die 8-gliedrigen Perioden sind Nullstellen des quadratischen Hilfspolynoms

$$(Y - \eta_{8,0}) \cdot (Y - \eta_{8,1}) = Y^2 - (\eta_{8,0} + \eta_{8,1}) \cdot Y + \eta_{8,0} \cdot \eta_{8,1}.$$

Nach Konstruktion ist $\eta_{8,0} + \eta_{8,1}$ die Summe aller Nullstellen von Φ_{17} , also -1 . Es kommt nun darauf an, die Teilmengen $\mathcal{N}_{8,0}$ und $\mathcal{N}_{8,1}$ so zu wählen, dass $\eta_{8,0} \cdot \eta_{8,1}$ eine ganze Zahl wird.

Gauss löst dieses Problem so. Die 16 Zahlen $1, 2, \dots, 15, 16$ sind modulo 17 kongruent mit den 16 Potenzen $3^0, 3^1, \dots, 3^{15}$ der Zahl 3 (siehe die folgende Tabelle).

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Gauss setzt $\mathcal{N}_{8,0}$ gleich der Menge der Nullstellen der Form $r^{3^{2\ell}}$; das Komplement $\mathcal{N}_{8,1}$ wird dann von den Nullstellen der Form $r^{3^{2\ell+1}}$ gebildet. Mit dieser Wahl werden die 8-gliedrigen Perioden zu

$$\begin{aligned} \eta_{8,0} &= r^1 + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2 \quad \text{und} \\ \eta_{8,1} &= r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6. \end{aligned}$$

Das Produkt $\eta_{8,0} \cdot \eta_{8,1}$ ist eine Summe von 64 Zahlen der Form $r^{3^{2k}} \cdot r^{3^{2\ell+1}} = r^{3^{2k} + 3^{2\ell+1}}$. Multipliziert man die Exponenten dieser Zahlen mit 3, ergeben sich die gleichen Zahlen; in der Tat ist $3 \cdot (3^{2k} + 3^{2\ell+1}) = 3^{2(j+1)} + 3^{2k+1}$. Ferner ist keiner dieser Exponenten ein Vielfaches von 17, denn aus $3^{2k} + 3^{2\ell+1} \equiv 0$ modulo 17 folgte

$$3^{2k} \equiv -3^{2\ell+1} \equiv 16 \cdot 3^{2\ell+1} \equiv 3^{2\ell+9} \pmod{17},$$

was zeigte, dass zwei der 16 Potenzen 3^n mit $n \in \{0, 1, \dots, 15\}$ kongruent waren. Daher ist $\eta_{8,0} \cdot \eta_{8,1}$ das Vierfache von $\sum_{k=1}^{16} r^k = -1$. Die 8-gliedrigen Perioden sind somit die Nullstellen des quadratischen Polynoms $f_{8,0} = Y^2 + Y - 4$.

Die Summe der beiden 4-gliedrigen Perioden $\eta_{4,0} = r + r^{13} + r^{16} + r^4$ und $\eta_{4,2} = r^9 + r^{15} + r^8 + r^2$ ist $\eta_{8,0}$; direkte Rechnung zeigt, dass ihr Produkt, eine Summe von 16 Zahlen, mit -1 übereinstimmt. Somit

sind $\eta_{4,0}$ und $\eta_{4,2}$ Nullstellen des Polynoms $f_{4,0} = Y^2 - \eta_{8,0} \cdot Y - 1$. Die Summe der 2-gliedigen Perioden $\eta_{2,0} = r + r^{16} = 2 \cos \frac{2\pi}{17}$ und $\eta_{2,4} = r^{13} + r^4 = 2 \cos \frac{8\pi}{17}$ ist $\eta_{4,0}$ und ihr Produkt berechnet sich zu

$$(r + r^{16}) \cdot (r^{13} + r^4) = r^{14} + r^5 + r^{29} + r^{20} = r^3 + r^5 + r^{12} + r^{14} = \eta_{4,1}.$$

Für die 4-gliedrige Periode $\eta_{4,1}$ braucht man noch das Hilfspolynom

$$f_{4,1} = (Y - \eta_{4,1}) \cdot (Y - \eta_{4,3}) = Y^2 - \eta_{8,1} \cdot Y + \eta_{4,1} \cdot \eta_{4,3} = Y^2 - \eta_{8,1} \cdot Y - 1.$$

Nach diesen Vorarbeiten fällt es leicht, einen Wurzelausdruck für $\eta_{2,0} = 2 \cos \frac{2\pi}{17}$ anzugeben. Zunächst ist $\eta_{8,0}$ eine Nullstelle des Polynoms $f_{8,0} = Y^2 + Y - 4$; da $\eta_{8,0} = 2\Re(r + r^9 + r^4 + r^2)$ positiv ist, haben die beiden 8-gliedrigen Perioden die Darstellungen $\eta_{8,0} = \frac{1}{2}(-1 + \sqrt{17})$ und $\eta_{8,1} = \frac{1}{2}(-1 - \sqrt{17})$. Die 4-gliedrige Periode $\eta_{4,0}$ ist eine Nullstelle von $f_{4,0} = Y^2 - \eta_{8,0} \cdot Y - 1$; da $\eta_{4,0} = 2\Re(r + r^{13}) > 2\Re(r^9 + r^{15}) = \eta_{4,2}$ ist, gilt

$$\eta_{4,0} = \frac{1}{2} \left(\eta_{8,0} + \sqrt{\eta_{8,0}^2 + 4} \right) = \frac{1}{4} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \right).$$

Ebenso berlegt man sich, dass die 4-gliedrige Periode $\eta_{4,1}$ die Beschreibung

$$\eta_{4,1} = \frac{1}{2} \left(\eta_{8,1} + \sqrt{\eta_{8,1}^2 + 4} \right) = \frac{1}{4} \left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}} \right)$$

hat. Die 2-gliedrige Periode $\eta_{2,0} = 2 \cos \frac{2\pi}{17}$ schliesslich ist eine Nullstelle des Polynoms $Y^2 - \eta_{4,0} \cdot Y + \eta_{4,1}$; die andere ist $\eta_{2,4} = 2\Re(r^4)$. Da $\eta_{2,4}$ kleiner als $\eta_{2,0}$ ist, ergeben sich für $\cos \frac{2\pi}{17}$ und $\cos \frac{8\pi}{17}$ die Ausdrücke $\frac{1}{4} \left(\eta_{4,0} + \sqrt{\eta_{4,0}^2 - 4\eta_{4,1}} \right)$ und $\frac{1}{4} \left(\eta_{4,0} - \sqrt{\eta_{4,0}^2 - 4\eta_{4,1}} \right)$. Fassen wir zusammen:

Satz 3. Um Ausdrücke zu finden für die x -Koordinaten der Ecken des regelmässigen 17-Eckes, das dem Einheitskreis einbeschrieben ist, berechne man erst

$$\begin{aligned} \eta_{8,0} &= \frac{1}{2} \left(-1 + \sqrt{1 + 16} \right), & \eta_{8,1} &= \frac{1}{2} \left(-1 - \sqrt{1 + 16} \right), \\ \eta_{4,0} &= \frac{1}{2} \left(\eta_{8,0} + \sqrt{\eta_{8,0}^2 + 4} \right) \text{ und } \eta_{4,1} = \frac{1}{2} \left(\eta_{8,1} + \sqrt{\eta_{8,1}^2 + 4} \right). \end{aligned}$$

Dann sind $\cos \frac{2\pi}{17} = \frac{1}{4} \left(\eta_{4,0} + \sqrt{\eta_{4,0}^2 - 4\eta_{4,1}} \right)$ und $\cos \frac{8\pi}{17} = \frac{1}{4} \left(\eta_{4,0} - \sqrt{\eta_{4,0}^2 - 4\eta_{4,1}} \right)$.

Diese Ausdrücke lassen sich unmittelbar in Konstruktionen mit Zirkel und Lineal bersetzen; $\eta_{8,0}$ und $\eta_{8,1}$ sind die x -Koordinaten der Schnittpunkte der x -Achse mit dem Kreis, der $(-1/2, 0)$ zum Mittelpunkt hat und $(0, 2)$ enthält; ähnlich gewinnt man die Punkte $(\eta_{4,0}, 0)$ und $(\eta_{4,1}, 0)$. Das Auffinden der Punkte $(\eta_{2,0}, 0)$ und $(\eta_{2,4}, 0)$ ist etwas komplizierter. (Eine zeichnerisch befriedigende Umsetzung der Ausdrücke findet sich im Buch [1] auf Seite 67.)

Interpretation der Gauss'schen Konstruktion im Rahmen der Theorie von Galois

Wie zuvor sollen Φ_{17} das Polynom $X^{16} + X^{15} + \dots + X + 1$ und $r = e^{2\pi i/17}, r^2, r^3, \dots, r^{16}$ seine Nullstellen bezeichnen. Das Polynom Φ_{17} ist in $\mathbb{Q}[X]$ unzerlegbar (Gauss, *Disquisitiones arithmeticae*, Art. 341). Dies impliziert, dass die 16 Nullstellen von Φ_{17} über \mathbb{Q} linear unabhängig sind; sie erzeugen also einen 16-dimensionalen, rationalen Unterraum $\mathbb{Q}[r]$ von \mathbb{C} . Dieser Unterraum enthält $1 = -(r + r^2 + \dots + r^{16})$, also alle Nullstellen des Polynoms $X^{17} - 1$. Da diese Nullstellen eine multiplikative Untergruppe bilden, ist $\mathbb{Q}[r]$ unter Produkten abgeschlossen und enthält das neutrale Element 1 der Multiplikation, ist also ein Unterring des Krpers der komplexen Zahlen. Aus dem erweiterten Euklidischen Algorithmus für Polynome ergibt sich noch, dass $\mathbb{Q}[r]$ sogar ein Krper ist; er ist isomorph zum Quotientenring $\mathbb{Q}[X]/(\mathbb{Q}[X] \cdot \Phi_{17})$.

Für jede der 16 Zahlen $k \in \{1, 2, \dots, 16\}$ kann die Zuordnung $r^\ell \mapsto r^{k \cdot \ell}$ zu einer linearen Abbildung $\sigma_k: \mathbb{Q}[r] \rightarrow \mathbb{Q}[r]$ fortgesetzt werden; sie ist bijektiv und mit der Multiplikation verträglich, also ein Automorphismus des Krpers $\mathbb{Q}[r]$. Da jeder Automorphismus von $\mathbb{Q}[r]$ die Nullstelle r auf eine andere Nullstelle von Φ_{17}

abbildet, machen die Abbildungen σ_k die ganze Automorphismengruppe des Krpers $\mathbb{Q}[r]$ aus. Der Umstand, dass die Zahlen $1, 2, 3, \dots, 16$ modulo 17 Potenzen von 3 sind, bedeutet nun, dass jeder Automorphismus σ_k eine Potenz des Automorphismus $\tau = \sigma_3$ ist. Die Automorphismengruppe $\text{Aut}(\mathbb{Q}[r])$ des Krpers $\mathbb{Q}[r]$ ist deshalb eine zyklische Gruppe der Ordnung 16, die vom Automorphismus τ erzeugt wird.

Weil die Gruppe $\text{Aut}(\mathbb{Q}[r])$ zyklisch ist und 16 Elemente entht, besitzt sie fr jeden Teiler von 16 genau eine Untergruppe. Die Untergruppe H_8 der Ordnung 8 wird von τ^2 erzeugt; die Menge der von ihr festgehaltenen Elemente bildet einen Teilkörper L^{H_8} von $L = \mathbb{Q}[r]$; er ist 2-dimensional. Die Gausssschen Perioden $\eta_{8,0}$ und $\eta_{8,1}$ liegen in diesem Teilkörper; da sie linear unabhngig sind, bilden sie eine Basis. Die Untergruppe H_4 der Ordnung 4 wird von τ^4 erzeugt; die Dimension ihres Fixkrpers L^{H_4} ist 4. Die 4-gliedrigen Gausssschen Perioden $\eta_{4,0}, \eta_{4,1}, \eta_{4,2}$ und $\eta_{4,3}$ liegen in diesem grsseren Teilkörper; sie sind linear unabhngig, bilden also eine Basis von L^{H_4} . Die Untergruppe H_2 der Ordnung 2 wird von τ^8 erzeugt; ihr Fixkörper hat Dimension 8 und die acht 2-gliedrigen Perioden $\eta_{2,0}, \dots, \eta_{2,7}$ bilden eine Basis dieses Teilkörpers.

Hinweise zur Literatur

Das gut lesbare und anregende Buch [12] von A. Weil behandelt das historische Umfeld und die Arbeiten zur Zahlentheorie der vier Mathematiker Fermat, Euler, Lagrange und Legendre. Insbesondere finden sich in den Abschnitten *Vollkommene Zahlen und der „kleine Satz von Fermat“* (pp. 52–60) und *Eulers Entdeckung der Zahlentheorie* (pp. 179–182) weitere Einzelheiten zum Thema dieses Aufsatzes. Das Buch [10] von P. Ribenboim entht einen Abschnitt ber Fermatsche Zahlen (Kap. 2, VI); in ihm werden ein Primzahltest fr diese Zahlen und Beispiele von Faktorisierungen dieser Zahlen besprochen. Einzelheiten zu neueren Faktorisierungen finden sich dann den Arbeiten [2], [9] und [14]. Im Artikel [13] schliesslich wird rekonstruiert, wie F. Landry im Jahre 1880 die Faktorisierung der Zahl F_6 gefunden haben knnte.

Was die Konstruierbarkeit des regelmssigen 17-Eckes angeht, so gibt Artikel 354 der 1801 erschienenen Gausssschen Werkes *Disquisitiones arithmeticae* eine Beschreibung der Konstruktion, welche auch heute noch gut verstndlich ist; die Darstellung in Bachmanns Buch [1] lehnt sich an sie eng an. Das Konstruktionsverfahren wird auch in verschiedenen Bchern ber Galois-Theorie behandelt, so in jenem von Stewart [11].

Abschliessend mchte ich noch auf ein Buch von I. N. Herstein und I. Kaplansky hinweisen [8]; ich habe es erst neulich entdeckt. Das Ziel der Autoren ist es *... to cover a selection of topics that give something of the flavor of modern mathematics. Furthermore, we try to carry each topic far enough to prove something substantial. Mastery of the material requires nothing beyond the algebra and geomertry normally covered in high school.* Abschnitt 2.9 dieses Buches behandelt Fermatsche und Mersennesche Zahlen.

- [1] P. BACHMANN: *Die Lehre von der Kreisteilung*; Teubner-Verlag, Leipzig 1872.
- [2] R. P. BRENT: *Factorization of the tenth Fermat number*; Math. Comp. **68** (1999), 429–541.
- [3] L. EULER: *Observationes de theoremate quodam FERMATIANO aliisque ad numeros primos spectantibus*; Comment. acad. sc. Petrop. **6** (1732/3), 1738, 103–107; in *Opera omnia*, series I, vol. 2, Abh. 26, pp. 1–5.
- [4] L. EULER: *Theoremata circa divisores numerorum*; Novi Comment. acad. sc. Petropolitanae **1** (1747/8), 1950, 20–48; in *Opera omnia*, series I, vol. 2, Abh. 134, pp. 62–85.
- [5] L. EULER: *Theoremata circa residua ex divisione potestatum relicta*; Novi comment. acad. sc. Petropolitanae **7** (1758/9), 1761, 49–82; in *Opera omnia*, series I, vol. 2, Abh. 262, pp. 493–518.
- [6] L. EULER: *De numeris amicabilibus*, unverffentlichtes Manuskript, verfasst um 1747; in *Opera omnia*, series I, vol. 5, Abh. 798, pp. 353–365.
- [7] C. F. GAUSS: *Untersuchungen ber hhere Arithmetik*; bersetzt von H. Maser; Springer-Verlag 1889.
- [8] I. N. HERSTEIN und I. KAPLANSKY: *Matters mathematical*; Chelsea Publishing Company 1978.
- [9] W. KELLER: *Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$* ; Math. Comp. **50** (1988), 261–263.
- [10] P. RIBENBOIM: *The book of prime number records*; Springer-Verlag 1988.
- [11] I. STEWART: *Galois Theorie*; Second edition, Chapman & Hall 1989.
- [12] A. WEIL: *Zahlentheorie*; Birkhuser-Verlag 1992.
- [13] H. C. WILLIAMS: *How was F_6 factored?*; Math. Comp. **61** (1993), 463–474.
- [14] J. YOUNG und D. A. BUELL: *The twentieth Fermat Number is composite*; Math. Comp. **41** (1983), 661–673.