Fermats letzter Satz

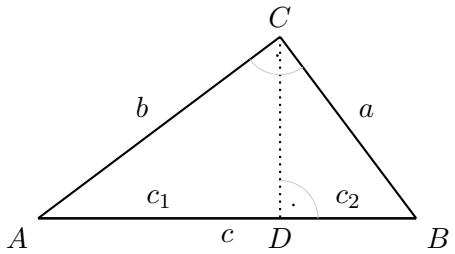
Benjamin Sambale*

7. März 2021

Satz 1 (Pythagoras)**.** *Ein Dreieck mit den Seitenlängen a, b und c ist genau dann rechtwinklig, wenn (bei geeigneter Beschriftung) $a^2 + b^2 = c^2$ gilt.*

Alle Beweise setzen gewisse geometrische Postulate voraus, die auf Euklids *Elemente* zurückgehen.

Beweis. Sei ABC ein rechtwinkliges Dreieck mit den Seiten a, b, c:



Die Dreiecke ABC und ADC haben neben dem rechten Winkel auch den Winkel an A gemeinsam. Sie sind daher ähnlich. Analog sind auch ABC und DBC ähnlich. Für die Seitenlängen gilt daher $\frac{a}{c} = \frac{c_2}{a}$ und $\frac{b}{c} = \frac{c_1}{b}$. Es folgt

$$a^2 + b^2 = cc_2 + cc_1 = c(c_1 + c_2) = c^2.$$

Seien nun a, b, c die Seitenlängen eines beliebigen Dreiecks Δ, sodass $a^2 + b^2 = c^2$ gilt. Sicher existiert ein rechtwinkliges Dreieck Δ' mit den Seitenlängen a, b, c', wobei c' die größte Seite ist. Nach dem ersten Teils des Beweises gilt $(c')^2 = a^2 + b^2 = c^2$ und somit $c' = c$. Also sind Δ und Δ' kongruent. Mit Δ' ist auch Δ rechtwinklig. □

Im Folgenden sei $\mathbb{N} = \{1, 2, \ldots\}$.

Definition 2. Man nennt $(a, b, c) \in \mathbb{N}^3$ ein *pythagoreisches Tripel*, falls $a^2 + b^2 = c^2$.

Beispiel 3. Offenbar sind $(3, 4, 5)$ und $(5, 12, 13)$ pythagoreische Tripel.

*Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany, sambale@math.uni-hannover.de

Satz 4 (EUKLID). *Jedes pythagoreische Tripel hat die Form*

$$d(2st, t^2 - s^2, t^2 + s^2) \qquad \text{oder} \qquad d(t^2 - s^2, 2st, t^2 + s^2)$$

wobei $d, s, t \in \mathbb{N}$ mit $s < t$. Umgekehrt liefert jede Wahl dieser Parameter ein pythagoreisches Tripel. Insbesondere gibt es unendlich viele pythagoreische Tripel.

Beweis. Sei (a, b, c) ein pythagoreisches Tripel und $d := \mathrm{ggT}(a, b)$. Dann ist d^2 ein Teiler von $a^2 + b^2 = c^2$. Nach der eindeutigen Primfaktorzerlegung ist d ein Teiler von c. Folglich ist auch $\frac{1}{d}(a, b, c)$ ein pythagoreisches Tripel. Wir können daher $\mathrm{ggT}(a, b) = 1$ annehmen. Insbesondere ist a oder b ungerade. Sind beide ungerade, so ergibt sich der Widerspruch $c^2 = a^2 + b^2 \equiv 2 \pmod 4$. O. B. d. A. sei also $a = 2k$ und b ungerade. Dann ist auch c ungerade und man erhält

$$\frac{c+b}{2}\frac{c-b}{2} = \frac{c^2 - b^2}{4} = \frac{a^2}{4} = k^2. \tag{1}$$

Sei $e \in \mathbb{N}$ ein gemeinsamer Teiler von $\frac{c+b}{2}$ und $\frac{c-b}{2}$. Dann teilt e auch $\frac{c+b}{2} + \frac{c-b}{2} = c$ sowie $\frac{c+b}{2} - \frac{c-b}{2} = b$. Folglich teilt e^2 auch $c^2 - b^2 = a^2$. Wegen $\mathrm{ggT}(a, b) = 1$ ist daher $e = 1$, d. h. $\frac{c+b}{2}$ und $\frac{c-b}{2}$ sind teilerfremd. Jeder Primfaktor von k teilt also entweder den ersten oder den zweiten Faktor in (1). Dies liefert $s, t \in \mathbb{N}$ mit $s < t$ und

$$\frac{c+b}{2} = t^2, \qquad \frac{c-b}{2} = s^2, \qquad st = k.$$

Wir berechnen

$$\begin{aligned} a &= 2k = 2st, \\ b &= \frac{c+b}{2} - \frac{c-b}{2} = t^2 - s^2, \\ c &= \frac{c+b}{2} + \frac{c-b}{2} = t^2 + s^2. \end{aligned}$$

Sind umgekehrt $d, s, t \in \mathbb{N}$ mit $s < t$ gegeben, so ist $(a, b, c) := d(2st, t^2 - s^2, t^2 + s^2) \in \mathbb{N}^3$ mit

$$a^2 + b^2 = d^2(4s^2t^2 + (t^2 - s^2)^2) = d^2(t^4 + 2s^2t^2 + s^4) = d^2(t^2 + s^2)^2 = c^2. \qquad \square$$

Wenn man zusätzlich $\mathrm{ggT}(s, t) = 1$ und $s \not\equiv t \pmod 2$ fordert, so sind die Zahlen d, s, t in Satz 4 eindeutig bestimmt.

Satz 5 (FERMATS „letzter“ Satz). *Für $n \geq 3$ existiert kein Tripel $(a, b, c) \in \mathbb{N}^3$ mit $a^n + b^n = c^n$.*

Bemerkung 6.

(i) Angenommen $a, b, c \in \mathbb{Z}$ erfüllen $a^n + b^n = c^n$. Ist n gerade oder $a, b, c < 0$, so gilt auch $|a|^n + |b|^n = |c|^n$. In allen anderen Fällen kann man notfalls c mit a oder b vertauschen, um $|a|^n + |b|^n = |c|^n$ zu erreichen. Fermats letzter Satz (kurz FLT) zeigt, dass mindestens eine der Zahlen a, b oder c Null sein muss. In $\mathbb{Z}^3$ gibt es daher nur *triviale* Lösungen. Das Gleiche gilt offenbar auch über $\mathbb{Q}$ (multipliziere mit gemeinsamen Nenner).

(ii) Ist Satz 5 für n bewiesen, so auch für nk mit $k \in \mathbb{N}$, denn jede Lösung $a^{nk} + b^{nk} = c^{nk}$ für nk liefert eine Lösung $(a^k)^n + (b^k)^n = (c^k)^n$ für n. Man braucht Satz 5 daher „nur“ für $n = 4$ und ungerade Primzahlen beweisen. Fermat hat seinen Satz nur für $n = 4$ bewiesen. Dies ist vermutlich der elementarste Fall.

Satz 7 (FERMAT)**.** *Es existiert kein Tripel* $(a,b,c) \in \mathbb{N}^3$ *mit* $a^4 + b^4 = c^4$.

Beweis. Nehmen wir etwas allgemeiner an, dass $(a,b,c) \in \mathbb{N}^3$ mit $a^4 + b^4 = c^2$ existieren (dies schließt die gegebene Gleichung ein wegen $c^4 = (c^2)^2$). Sei dabei c so klein wie möglich. Dann gilt $\mathrm{ggT}(a,b) = 1$, denn anderenfalls könnte man wie im Beweis von Satz 4 durch $\mathrm{ggT}(a,b)$ teilen. Da (a^2, b^2, c) ein pythagoreisches Tripel ist, existieren $s, t \in \mathbb{N}$ mit $s < t$ und o. B. d. A. $(a^2, b^2, c) = (2st, t^2 - s^2, t^2 + s^2)$. Nun ist auch (b, s, t) ein pythagoreisches Tripel mit $\mathrm{ggT}(b,s) \mid \mathrm{ggT}(b, 2st) = \mathrm{ggT}(b, a^2) = 1$. Da a gerade ist, ist b ungerade. Nach Satz 4 existieren also $u, v \in \mathbb{N}$ mit $(b, s, t) = (v^2 - u^2, 2uv, v^2 + u^2)$. Wegen $\mathrm{ggT}(a,b) = 1$ ist auch $\mathrm{ggT}(s,t) = 1$. Dabei ist $s = 2uv$ gerade und t ist ungerade. Die Primfaktorzerlegung von $a^2 = 2st$ zeigt $s = 2x^2$ und $t = y^2$ mit $x, y \in \mathbb{N}$ und $\mathrm{ggT}(x,y) = 1$. Schließlich gilt auch $\mathrm{ggT}(u,v) \mid \mathrm{ggT}(b,s) = 1$. Die Gleichung $x^2 = uv$ liefert daher $p, q \in \mathbb{N}$ mit $u = p^2$ und $v = q^2$. Insgesamt erhält man $p^4 + q^4 = u^2 + v^2 = t = y^2$ mit $y \leq y^2 = t \leq t^2 < t^2 + s^2 = c$. Dies widerspricht der Wahl von (a,b,c). □

Nach Bemerkung 6 und Satz 7 genügt es FLT für jede ungerade Primzahl $n = p$ zu beweisen. Die Idee ist die Summe $a^p + b^p$ in ein Produkt zu verwandeln und anschließend mit der Primfaktorzerlegung von c^p zu vergleichen. Sei dazu $\zeta := e^{2\pi \mathrm{i}/p} \in \mathbb{C}$. Da p ungerade ist, sind $-\zeta, -\zeta^2, \ldots, -\zeta^p = 1$ die Nullstellen von $X^p + 1$, d. h.

$$X^p + 1 = \prod_{i=1}^{p} (X + \zeta^i).$$

Wir substituieren $\frac{a}{b}$ für X und multiplizieren anschließend mit b^p:

$$a^p + b^p = \prod_{i=1}^{p} (a + \zeta^i b). \tag{2}$$

Die Faktoren auf der rechten Seite sind leider keine ganzen Zahlen mehr. Wir rechnen daher im größeren Ring

$$R := \mathbb{Z}[\zeta] := \{a_2 \zeta^{p-2} + a_3 \zeta^{p-3} + \ldots + a_p : a_2, \ldots, a_p \in \mathbb{Z}\}$$

(wegen $1 + \zeta + \ldots + \zeta^{p-1} = \frac{\zeta^p - 1}{\zeta - 1} = 0$ ist R tatsächlich ein Teilring des Kreisteilungskörpers $\mathbb{Q}(\zeta) = \mathbb{Q}_p \subseteq \mathbb{C}$). Wie in $\mathbb{Z}$ schreibt man $\alpha \mid \beta$ oder $\beta \equiv 0 \pmod{\alpha}$ für $\alpha, \beta \in R$, falls ein $\gamma \in R$ mit $\alpha\gamma = \beta$ existiert.

Definition 8.

(i) Für $\alpha \in R$ sei

$$\mathrm{N}(\alpha) := \prod_{\Gamma \in \mathrm{Gal}(\mathbb{Q}_p | \mathbb{Q})} \Gamma(\alpha) \in \mathbb{C}$$

die *Norm* von α.

(ii) Ein Element $\alpha \in R \setminus \{0\}$ heißt *invertierbar*, falls $\alpha^{-1} \in R$ (als komplexe Zahl). Die invertierbaren Elemente von R bilden die *Einheitengruppe* $R^\times$.

(iii) Ein Element $\alpha \in R \setminus (R^\times \cup \{0\})$ heißt *irreduzibel*, falls es keine Faktorisierung $\alpha = \beta\gamma$ mit $\beta, \gamma \in R \setminus R^\times$ gibt.

(iv) Man nennt $\alpha, \beta \in R$ *assoziiert*, falls $\epsilon \in R^\times$ mit $\alpha = \epsilon\beta$ existiert. Gegebenenfalls schreibt man $\alpha \sim \beta$.

Lemma 9. *Für* $\alpha, \beta \in R$ *gilt:*

(i) $\mathrm{N}(\alpha) = 0 \iff \alpha = 0$.

(ii) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

(iii) $\mathrm{N}(\alpha) \in \mathbb{N}_0$.

(iv) $R^\times = \{\alpha \in R : \mathrm{N}(\alpha) = 1\}$.

(v) Ist $\mathrm{N}(\alpha)$ *eine Primzahl, so ist* α *irreduzibel.*

Beweis.

(i,ii) Trivial.

(iii) Für $\Gamma \in \mathrm{Gal}(\mathbb{Q}_p|\mathbb{Q}) =: \mathcal{G}$ existiert $k \in \mathbb{Z}$ mit $\Gamma(\zeta) = \zeta^k$. Dies zeigt $\mathrm{N}(\alpha) \in R$. Sei also $\mathrm{N}(\alpha) = a_2\zeta^{p-2} + a_3\zeta^{p-3} + \ldots + a_p$ mit $a_2, \ldots, a_p \in \mathbb{Z}$. Da $\mathbb{Q} \subseteq \mathbb{Q}_p$ eine Galois-Erweiterung ist, gilt $\mathrm{N}(\alpha) \in \mathbb{Q}_p^{\mathcal{G}} = \mathbb{Q}$. Da $1, \zeta, \ldots, \zeta^{p-2}$ linear unabhängig über $\mathbb{Q}$ sind, folgt $\mathrm{N}(\alpha) = a_p \in \mathbb{Z}$. Wegen $\zeta \notin \mathbb{R}$ ist die komplexe Konjugation ein nicht-trivialer Automorphismus auf $\mathbb{Q}_p$. Man kann die Faktoren von $\mathrm{N}(\alpha)$ daher in Paaren der Form $\Gamma(\alpha)\overline{\Gamma(\alpha)} = |\Gamma(\alpha)|^2 \geq 0$ anordnen. Dies liefert $\mathrm{N}(\alpha) \geq 0$.

(iv) Für $\alpha \in R$ gilt $1 = \mathrm{N}(1) = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(\alpha)\mathrm{N}(\alpha^{-1})$. Wegen $\mathrm{N}(\alpha), \mathrm{N}(\alpha^{-1}) \in \mathbb{N}_0$ folgt $\mathrm{N}(\alpha) = 1$. Ist umgekehrt $\mathrm{N}(\alpha) = 1$, so ist $\alpha^{-1} = \prod_{i=1}^{p-2} \Gamma^i(\alpha) \in R$.

(v) Sei $\mathrm{N}(\alpha) = p$ eine Primzahl. Nach (i,ii) ist $\alpha \neq 0$ keine Einheit. Sei $\alpha = \beta\gamma$ mit $\beta, \gamma \in R$. Dann gilt $p = \mathrm{N}(\beta)\mathrm{N}(\gamma)$ und (iii) zeigt $\beta \in R^\times$ oder $\gamma \in R^\times$. □

Offenbar ist $\sim$ eine Äquivalenzrelation auf R. Sei P ein Repräsentantensystem für die nicht-assoziierten irreduziblen Elemente (das Analogon zur Menge der (positiven) Primzahlen in $\mathbb{Z}$). Durch Induktion nach der Norm sieht man, dass jedes $\alpha \in R \setminus \{0\}$ eine Faktorisierung der Form

$$\alpha = \epsilon \prod_{\pi \in P} \pi^{a_\pi}$$

mit $\epsilon \in R^\times$ und $a_\pi \geq 0$ für $\pi \in P$ besitzt. Sind die Zahlen ϵ und a_π dabei eindeutig bestimmt, so nennt man R *faktoriell* (d. h. es gibt eine eindeutige „Primfaktorzerlegung“). In diesem Fall definiert man

$$\mathrm{ggT}(\alpha, \beta) = \prod_{\pi \in P} \pi^{\min(a_\pi, b_\pi)}$$

für $\beta = \epsilon' \prod_{\pi \in P} \pi^{b_\pi}$. Im Fall $\mathrm{ggT}(\alpha, \beta) \in R^\times$ nennt man α und β teilerfremd.

Ab jetzt beschränken wir uns auf $p = 3$. Es gilt dann $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ und $\zeta^2 + \zeta + 1 = 0$. Für $\alpha = a + b\zeta \in R$ ist

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = |\alpha|^2 = (a + b\zeta)(a + b\zeta^2) = a^2 + b^2 - ab.$$

Insbesondere ist $R^\times = \{\alpha \in R : |\alpha| = 1\}$. Für $\alpha \neq 0$ ist $|\alpha| = \sqrt{\mathrm{N}(\alpha)} \geq 1$. Aus $\beta \mid \alpha$ folgt also $|\beta| \leq |\alpha|$. Nach Algebra 2 ist R bzgl. der Norm euklidisch und daher faktoriell. Wir betrachten $\lambda := 1 - \zeta$. Wegen $\mathrm{N}(\lambda) = 3$ ist λ irreduzibel. Wegen $\zeta \equiv 1 \pmod{\lambda}$ gilt $R/(\lambda) \cong \mathbb{F}_3$.

Lemma 10. *Für* $\alpha \in R$ *mit* $\lambda \nmid \alpha$ *gilt* $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.

Beweis. Indem man notfalls α durch $-\alpha$ ersetzt, kann man $\alpha \equiv 1 \pmod{\lambda}$ annehmen. Sei $\beta \in R$ mit $\alpha - 1 = \beta\lambda$. Dann gilt

$$\begin{aligned}\alpha - \zeta &= (\alpha - 1) + \lambda = \lambda(\beta + 1),\\ \alpha - \zeta^2 &= (\alpha - \zeta) + (\zeta - \zeta^2) = \lambda(\beta + 1) + \zeta\lambda = \lambda(\beta - \zeta^2).\end{aligned}$$

Es folgt

$$\alpha^3 - 1 = (\alpha - 1)(\alpha - \zeta)(\alpha - \zeta^2) = \lambda^3\beta(\beta + 1)(\beta - \zeta^2).$$

Wegen $\zeta^2 \equiv 1 \pmod{\lambda}$ liegen β, $\beta + 1$ und $\beta - \zeta^2$ in verschiedenen Restklassen modulo λ. Eine der Zahlen muss daher durch λ teilbar sein. Dies zeigt die Behauptung. □

Satz 11 (Euler)**.** *Es gibt kein Tripel* $(a, b, c) \in \mathbb{N}^3$ *mit* $a^3 + b^3 = c^3$.

Beweis. Wir nehmen allgemeiner an, dass $\alpha, \beta, \gamma \in R\setminus\{0\}$ mit $\alpha^3+\beta^3 \sim \gamma^3$ existieren. O. B. d. A. seien α, β und γ (paarweise) teilerfremd. Sei $\epsilon \in R^\times$ mit $\alpha^3 + \beta^3 = \epsilon\gamma^3$. Nehmen wir zunächst $\lambda \mid \alpha\beta$ an. O. B. d. A. sei $\lambda \mid \alpha$ und $\lambda \nmid \beta$ sowie $\lambda \nmid \gamma$. Nach Lemma 10 ist dann $\pm\epsilon \equiv \epsilon\gamma^3 = \alpha^3+\beta^3 \equiv \pm 1 \pmod{\lambda^2}$ und $\lambda^2 \mid 1 \pm \epsilon$. Im Fall $\epsilon \neq \mp 1$ wäre $3 = |\lambda^2| \leq |1 \pm \epsilon| \leq 2$ nach der Dreiecksungleichung. Also ist $\epsilon = \mp 1$ und $\beta^3 + (\pm\gamma)^3 = (-\alpha)^3$. Durch Vertauschen von α und γ kann man also $\lambda \nmid \alpha\beta$ annehmen.

Unter allen solchen Gegenbeispielen wählen wir γ, sodass

$$t := \nu(\gamma) := \max\{n \in \mathbb{N}_0 : \lambda^n \mid \gamma\}$$

möglichst klein ist. Im Fall $t = 0$ existieren $e, f \in \{\pm 1\}$ mit

$$\pm\epsilon \equiv \gamma^3 = \alpha^3 + \beta^3 \equiv e + f \pmod{\lambda^4}$$

nach Lemma 10. Offenbar ist $e = f$ und $\lambda^4 \mid \epsilon \pm 2$. Dies liefert den Widerspruch $9 = |\lambda^4| \leq |\epsilon \pm 2| \leq 5$. Im Fall $t = 1$ ist

$$0 \not\equiv \epsilon\gamma^3 = \alpha^3 + \beta^3 \equiv \pm 2 \pmod{\lambda^4}$$

und $\lambda \mid \epsilon\gamma^3 + (\pm 2 - \epsilon\gamma^3) = \pm 2$. Dies ergibt den Widerspruch $3 = \mathrm{N}(\lambda) \mid \mathrm{N}(2) = 4$. Also ist $t \geq 2$ und $\nu(\gamma^3) = 3t \geq 6$.

Gleichung 2 wird zu

$$(\alpha + \beta)(\alpha + \beta\zeta)(\alpha + \beta\zeta^2) = \epsilon\gamma^3. \tag{3}$$

Es folgt $\nu(\alpha + \beta) \geq 2$, $\nu(\alpha + \beta\zeta) \geq 2$ oder $\nu(\alpha + \beta\zeta^2) \geq 2$. O. B. d. A. sei $\nu(\alpha + \beta) \geq 2$ (anderenfalls ersetze man β durch $\beta\zeta$ bzw. $\beta\zeta^2$). Wegen $\lambda \nmid \beta$ ist dann

$$\begin{aligned}\nu(\alpha + \beta\zeta) &= \nu(\alpha + \beta - \beta(1 - \zeta)) = \nu(\alpha + \beta - \beta\lambda) = 1,\\ \nu(\alpha + \beta\zeta^2) &= \nu(\alpha + \beta - \beta\lambda(1 + \zeta)) = \nu(\alpha + \beta + \beta\lambda\zeta^2) = 1.\end{aligned}$$

Dies zeigt $\nu(\alpha + \beta) = 3t - 2 \geq 4$. Sei $\delta \not\sim \lambda$ irreduzibel. Ist δ ein gemeinsamer Teiler von $\alpha + \beta$ und $\alpha + \beta\zeta$, so teilt δ auch $\beta(1 - \zeta) = \beta\lambda$. Es folgt $\delta \mid \beta$ und $\delta \mid \alpha$ im Widerspruch zu $\mathrm{ggT}(\alpha, \beta) \in R^\times$. Analog sieht man, dass δ höchstens eine der Zahlen $\alpha + \beta$, $\alpha + \beta\zeta$ und $\alpha + \beta\zeta^2$ teilen kann. Die Primfaktorzerlegung von (3) liefert daher $\alpha_1, \beta_1, \rho \in R$ und $\epsilon_1, \epsilon_2, \epsilon_3 \in R^\times$ mit

$$\alpha + \beta = \epsilon_1\lambda^{3t-2}\rho, \qquad \alpha + \beta\zeta = \epsilon_2\lambda\alpha_1^3, \qquad \alpha + \beta\zeta^2 = \epsilon_3\lambda\beta_1^3$$

und $\lambda \nmid \alpha_1\beta_1$. Es folgt

$$0 = (\alpha + \beta) + (\alpha + \beta\zeta)\zeta + (\alpha + \beta\zeta^2)\zeta^2 = \epsilon_1\lambda^{3t-2}\rho^3 + \epsilon_2\lambda\alpha_1^3\zeta + \epsilon_3\lambda\beta_1^3\zeta^2.$$

Wir setzen $\gamma_1 := \lambda^{t-1}\rho$. Dann existieren $\mu_1, \mu_2 \in R^\times$ mit

$$\alpha_1^3 + \mu_1\beta_1^3 = \mu_2\gamma_1^3.$$

Wegen $t \geq 2$ ist $\lambda \mid \gamma_1$ und daher $0 \equiv \mu_2\gamma_1^3 \equiv 1 \pm \mu_1 \pmod{\lambda^2}$ nach Lemma 10. Wie oben folgt $\mu_1 = \mp 1$. Daher ist

$$\alpha_1^3 + (\mp\beta_1)^3 = \mu_2\gamma_1^3$$

mit $\nu(\gamma_1) = t - 1$ im Widerspruch zur Wahl von γ. □

Bemerkung 12.

(i) Legrendre und Dirichlet bewiesen FLT für $p = 5$.

(ii) Lamé hatte geglaubt obigen Beweis für alle $p > 2$ führen zu können. Liouville wies aber daraufhin, dass R für $p > 19$ nicht mehr faktoriell ist. Für $p = 23$ sind beispielsweise

$$6 = 2 \cdot 3 = \frac{1 + \sqrt{-23}}{2} \cdot \frac{1 - \sqrt{-23}}{2}$$

zwei verschiedene Faktorisierungen in irreduzible Elemente.

(iii) Als Alternative zeigte Kummer, dass zumindest alle *Ideale* in R eine eindeutige Faktorisierung in Primideale besitzen (Ringe mit dieser Eigenschaft heißen *Dedekind-Ringe*). Mittels der *Klassenzahl* lässt sich genau messen, wie weit R von einem faktoriellen Ring entfernt ist. Kummer bewies FLT für *reguläre* Primzahlen p, d. h. die Klassenzahl von R ist nicht durch p teilbar. Diese Primzahlen $p > 2$ lassen sich äquivalent dadurch charakterisieren, dass die Zähler der Bernoulli-Zahlen $B_2, B_4, \ldots, B_{p-3}$ nicht durch p teilbar sind. Die Bernoulli-Zahlen treten als Koeffizienten der Potenzreihe

$$\frac{X}{\exp(X) - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n$$

auf und lassen sich durch die Rekursionsformel

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

mit dem Startwert $B_0 = 1$ berechnen. Es gilt $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$ und $B_{2n+1} = 0$ für $n \geq 1$ (Der *Nenner* von B_{2n} ist das Produkt aller Primzahlen q mit $q - 1 \mid 2n$ nach Clausen und von Staudt). Damit gilt FLT für $p \leq 31$. Leider hat Jensen gezeigt, dass es unendlich viele *irreguläre* Primzahlen gibt (wobei $p = 37$ die kleinste ist).

(iv) Betrachtet man $a^3 + b^3 = c^3$ modulo 9, so sieht man $p \mid abc$ (dies entspricht der Behauptung $t \geq 1$ im Beweis von Satz 11). Für $p > 3$ ist diese Schlussweise nicht möglich. Man unterscheidet daher zwischen dem *ersten Fall* ($p \nmid abc$) und dem *zweiten Fall* ($p \mid abc$). Im ersten Fall sind die Hauptideale in der Faktorisierung

$$(c)^p = \prod_{i=1}^{p} (a + b\zeta)$$

aus Gleichung 2 teilerfremd. Jedes der Ideale $(a + b\zeta^i)$ ist daher die p-te Potenz eines Ideals. Ist p regulär, so ist $(a + b\zeta^i)$ sogar die p-te Potenz eines Hauptideals. Dies erlaubt eine ähnliche Argumentation wie in Satz 11. Germain hat den ersten Fall für alle Primzahlen p bewiesen, für die auch $2p + 1$ eine Primzahl ist (sogenannte *Germain-Primzahlen*).

(v) Faltings bewies, dass bei festem p nur höchstens endlich viele teilerfremde Lösungen (a, b, c) existieren können.

(vi) 1993 legte Wiles einen 100-seitigen Beweis für FLT in voller Allgemeinheit vor. Dieser enthielt jedoch eine Lücke, die Wiles zusammen mit Taylor ein Jahr später schließen konnte. Im Beweis interpretiert man FLT als elliptische Kurve und benutzt modulare Formen.

(vii) Für $p = 3$ und $\alpha = a + b\zeta \in R$ ist

$$\mathrm{N}(\alpha) = a^2 + b^2 - ab = \frac{1}{2}(a-b)^2 + \frac{1}{2}a^2 + \frac{1}{2}b^2.$$

Eine einfache Fallunterscheidung zeigt $R^\times = \langle -\zeta \rangle = \{\pm 1, \pm\zeta, \pm\zeta^2\}$. Für $p > 3$ ist jedoch $|R^\times| = \infty$ nach *Dirichlets Einheitensatz*. Für $p = 5$ ist beispielsweise $\epsilon = \sqrt{5} + 2 \in R^\times$ mit $\epsilon^{-1} = \sqrt{5} - 2$ und $\epsilon^n \to \infty$ für $n \to \infty$.