Fermats Vermutung für Exponent 3

Wir wollen zeigen, dass die Gleichung

$$a^3 + b^3 + c^3 = 0$$

keine Lösung $a, b, c \in \mathbb{Z} \setminus \{0\}$ hat.
Man kann leicht einsehen, dass auf jeden Fall aus jeder ganzzahligen Lösung der Gleichung eine Lösung mit paarweise teilerfremden Zahlen a, b, c gemacht werden kann (Division durch gemeinsame Teiler), und dass einer der drei Summanden durch 3 teilbar ist (löse die Gleichung modulo 9).
Ohne Einschränkung legen wir fest, dass c durch 3 teilbar sein soll, und schreiben $c = 3^k \cdot \tilde{c}$, wobei $\tilde{c}$ nicht durch 3 teilbar ist. Dann bekommen wir die Gleichung

$$a^3 + b^3 = 3^{3k} \cdot (-\tilde{c})^3.$$

Das Ärgernis an dieser Gleichung ist, dass links eine Summe steht und rechts ein Produkt. Man möchte gerne die linke Seite in ein Produkt umwandeln, um sie besser gegen die rechte Seite ausspielen zu können. Dazu benutzen wir die komplexe Zahl $\zeta = \frac{1}{2}(-1+\sqrt{-3})$. Sie ist eine Nullstelle des dritten Kreisteilungspolynoms $\Phi_3(X) = X^2 + X + 1$, also eine primitive dritte Einheitswurzel. Mit ihr können wir die linke Seite schreiben als

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2) = (a+b) \cdot (a+\zeta b) \cdot (a+\zeta^2 b).$$

Aber nun sind wir außerhalb von $\mathbb{Z}$ gelandet, und müssen in einem größeren Ring rechnen, nämlich in $\mathcal{O} := \mathbb{Z}[\zeta]$. Das ist der Ganzheitsring von $\mathbb{Q}(\sqrt{-3})$, und wir wissen sogar, dass er euklidisch ist. In $\mathcal{O}$ ist 3 kein Primelement mehr, es gilt

$$3 = -\zeta(1-\zeta)^2.$$

Allerdings ist $1-\zeta$ irreduzibel, denn seine Norm ist 3 (also eine Primzahl), und damit ist $1-\zeta$ im euklidischen Ring $\mathcal{O}$ sogar prim.
Wir schreiben nun flugs die Fermat-Gleichung um zu

$$(a+b) \cdot (a+\zeta b) \cdot (a+\zeta^2 b) = \zeta^{3k}(1-\zeta)^{3\cdot(2\cdot k)}(\tilde{c})^3.$$

Dabei sind $a, b, \tilde{c}$ teilerfremd zu $1-\zeta$, denn ihre Norm ist nicht durch $3 = \mathcal{N}(1-\zeta)$ teilbar.
Statt nun die ursprüngliche Gleichung von Fermat zu behandeln, zeigen wir das Folgende:
In $\mathcal{O}$ gibt es keine teilerfremden Elemente $a, b, c \in \mathcal{O} \setminus (1-\zeta)\mathcal{O}$, sodass

$$a^3 + b^3 = \epsilon \cdot (1-\zeta)^{3m} \cdot c^3$$

für eine Einheit $\epsilon \in \mathcal{O}^\times$ und eine natürliche Zahl m gilt.
Um dies zu zeigen nehmen wir an, es gäbe solche Elemente $a, b, c \in \mathcal{O} \setminus (1-\zeta)\mathcal{O}$. Diese können wir dann auch so wählen, dass das benötigte $m \in \mathbb{N}$ so klein wie möglich ist.
Wir zeigen dann, dass wir m noch weiter verkleinern können, und erhalten damit einen Widerspruch. Das geht jetzt so:
Wir schreiben die linke Seite wieder als

$$(a+b)(a+\zeta b)(a+\zeta^2 b).$$

$1-\zeta$ teilt die rechte Seite, denn $m \geq 1$. Da dies ein Primelement ist, teilt es auch einen Faktor der linken Seite. Andererseits sind diese Faktoren modulo $1-\zeta$ alle kongruent:

$$a + b\zeta = a + b - b(1-\zeta) = a + \zeta^2 b + \zeta b(1-\zeta),$$

und deshalb teilt $1-\zeta$ alle Faktoren auf der linken Seite.
Andererseits ist die Differenz von je zwei der Faktoren auf der linken Seite niemals durch 3 teilbar. Wäre zum Beispiel $(a+b)-(a+\zeta b) = (1-\zeta)b$ durch $3 = -\zeta(1-\zeta)^2$ teilbar, so wäre auch b durch $(1-\zeta)$ teilbar, was aber verboten ist. Analog argumentiert man für die anderen Paare von Faktoren auf der linken Seite. Das heißt, dass die Differenzen der Elemente $(a+\zeta^i b)/(1-\zeta) \in \mathcal{O},\ 0 \leq i \leq 2$, nicht durch $(1-\zeta)$ teilbar sind. Wir schreiben diese Elemente als $(a+\zeta^i b)/(1-\zeta) = x_i + y_i\zeta,\ x_i, y_i \in \mathbb{Z}$. Dann sind die Zahlen $\mathbb{Z} \ni x_i + y_i = x + y_i\zeta + y_i(1-\zeta)$ paarweise modulo 3 verschieden, da sonst ihre Differenz durch $1-\zeta$ teilbar wäre. Also ist genau eine der Zahlen $x_i + y_i$ in $\mathbb{Z}$ durch drei teilbar.
Folglich ist genau eine der drei Zahlen $(a+\zeta^i b)/(1-\zeta) \in \mathcal{O},\ 0 \leq i \leq 2$, durch $1-\zeta$ teilbar.
Indem wir notfalls b mit einer Potenz von ζ multiplizieren, dürfen wir annehmen, dass $a+b$ durch $(1-\zeta)^2$, also durch 3, teilbar ist, die anderen Faktoren aber nur einmal durch $1-\zeta$. Insbesondere muss $m > 1$ gelten, was wir gleich noch brauchen, damit auch $m-1$ noch eine natürliche Zahl ist.
Nun schreiben wir

$$a + b = (1-\zeta)^{3m-2} c_0,\ a + \zeta b = (1-\zeta)c_1, a + \zeta^2 b = (1-\zeta)c_2.$$

Dabei sind die Elemente $c_0, c_1, c_2 \in \mathcal{O}$ paarweise teilerfremd. Denn ein gemeinsamer Primteiler z.B. von $a+b$ und $a+\zeta b$ teilte auch $a+b-(a+\zeta b) = (1-\zeta)b$, und wäre er auch ein Teiler von b, so auch von $a+b-b = a$, was wegen der Teilerfremdheit dieser beiden verboten ist. Also muss der Primteiler $1-\zeta$ teilen, was selbst schon prim ist, und ist damit kein Teiler von $c_0 = (a+b)/(1-\zeta)^{3m-2}$.

Das Produkt der c_i ist (bis auf den Faktor ϵ) eine dritte Potenz in $\mathcal{O}$. Da $\mathcal{O}$ euklidisch ist und die c_i paarweise teilerfremd, muss jedes der c_i bis auf eine Einheit selbst schon eine dritte Potenz in $\mathcal{O}$ sein:

$$c_i = \epsilon_i \cdot d_i^3, \epsilon_i \in \mathcal{O}^\times, d_i \in \mathcal{O}.$$

Damit findet sich die folgende Identität:

$$(a+\zeta b)(1-\zeta)^{3(m-1)} = (a+b)\frac{d_1^3}{d_0^3}\frac{\epsilon_1}{\epsilon_0}, \quad (a+\zeta^2 b)(1-\zeta)^{3(m-1)} = (a+b)\frac{d_2^3}{d_0^3}\frac{\epsilon_2}{\epsilon_0}.$$

Andererseits gilt

$$(a+\zeta b)(1+\zeta) - (a+\zeta^2 b) = \zeta(a+b).$$

Dies multiplizieren wir mit $(1-\zeta)^{3(m-1)}$ und ersetzen die Ausdrücke links durch die eben gelernten Identitäten. Nach Kürzen von $(a+b)$ folgt

$$\frac{d_1^3}{d_0^3}\frac{\epsilon_1}{\epsilon_0}(1+\zeta) - \frac{d_2^3}{d_0^3}\frac{\epsilon_2}{\epsilon_0} = \zeta(1-\zeta)^{3(m-1)}.$$

Wenn wir hier wiederum mit d_0^3 multipliziert und durch die Einheit $\frac{\epsilon_1}{\epsilon_0}(1+\zeta)$ geteilt haben, so bekommen wir die Gleichung

$$d_1^3 + \varepsilon_1 d_2^3 = \varepsilon_2(1-\zeta)^{3(m-1)} d_0^3.$$

Dabei sind $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^\times$, und das m ist um eins kleiner als in unserer Ausgangsgleichung.
Um allerdings wirklich den gewünschten Widerspruch zur Minimalität von m in der Ausgangsgleichung zu bekommen, müssen wir noch den störenden Faktor ε_1 auf der rechten Seite loswerden.
Wir zeigen dazu, dass $\varepsilon_1 = \pm 1$ gilt und damit in das d_1^3 gezogen werden kann.
Um dies zu bewerkstelligen merken wir erst einmal an, dass ε_1 modulo 3 eine dritte Potenz ist. Wir können nämlich wegen der Euklidizität von $\mathcal{O}$ ein $\delta \in \mathcal{O}$ wählen, sodass $(1-\zeta)^2 \mid (\delta d_2 - 1)$, und dann folgt

$$\varepsilon_1 \equiv (-d_1\delta)^3 \pmod{(1-\zeta^2)}.$$

Modulo $1-\zeta$ können wir $(-d_1\delta)$ durch $l \in \{0,1,2\}$ ersetzen, d.h. $(-d_1\delta) = l + (1-\zeta)r,\ r \in \mathcal{O}$.
Dann folgt

$$\varepsilon_1 \equiv (-d_1\delta)^3 \equiv (l+(1-\zeta)r)^3 \equiv l^3 \pmod{3}.$$

Die Einheiten in $\mathcal{O}$ sind aber gerade die Elemente

$$1, \zeta, \zeta^2, -1, -\zeta, -\zeta^2,$$

und davon können nur ± 1 modulo 3 zur natürlichen Zahl l^3 kongruent sein. Damit ist aber $\varepsilon_1 \in \{\pm 1\}$ gezeigt.

Bemerkung. Es gibt vielleicht auch kürzere Beweise der gewünschten Aussage, aber dieser hier birgt in sich die Möglichkeit der Verallgemeinerung auf andere Fälle der Fermat-Gleichung.

Konkreter: wenn $p > 2$ eine Primzahl ist und $\zeta = \cos\frac{2\pi}{p} + \mathrm{i}\sin\frac{2\pi}{p}$ eine primitive p-te Einheitswurzel, dann ist im Ring

$$\mathbb{Z}[\zeta] := \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Z}\}$$

die Zahl p assoziiert zu $(1-\zeta)^{p-1}$. Andererseits gilt

$$a^p + b^p = (a+b)\cdot(a+\zeta b)\cdot(a+\zeta^2 b)\cdot\ldots\cdot(a+\zeta^{p-1}b),$$

und man kann diese Produktzerlegung benutzen, um zu zeigen, dass es keine Lösung der Fermat-Gleichung gibt mit $p \mid c$, wenn der Ring $\mathbb{Z}[\zeta]$ ein Hauptidealring ist. Das geht fast genauso wie hier im Fall $p = 3$ vorgerechnet.
Von Kummer stammt eine noch viel subtilere Bedingung an p, die solch ein Vorgehen rechtfertigt, nämlich die Bedingung, dass p „regulär“ sein soll. Das bedeutet, dass p kein Teiler der Klassenzahl von $\mathbb{Z}[\zeta]$ ist (was ich hier nicht näher erläutere). Letztlich habe ich den hier vorgeführten Beweis durch Elementarisierung des Kummerschen Beweises gewonnen.
Es ist allerdings noch immer unklar, ob es unendlich viele reguläre Primzahlen gibt, während z.B. bekannt ist, dass unendlich viele Primzahlen nicht regulär sind. Die kleinste irreguläre Primzahl ist 37.