Euler's proof of Fermat's Last Theorem for the exponent three

Dietmar A. Salamon
ETH-Zürich

12 March 2025

1 Eisenstein integers

Define the complex number ω by

$$\omega := \exp(2\pi\mathbf{i}/3) = -\frac{1}{2} + \frac{\mathbf{i}}{2}\sqrt{3} \in \mathbb{C}$$

so that $\omega \neq 1$, $\overline{\omega} = \omega^2 = \omega^{-1}$, and

$$\omega^3 = 1, \qquad 1 + \omega + \omega^2 = 0. \tag{1}$$

The **ring of Eisenstein integers** is the set $\Lambda \subset \mathbb{C}$ defined by

$$\Lambda := \left\{u + v\omega \,\middle|\, u, v \in \mathbb{Z}\right\} = \left\{\frac{k}{2} + \frac{\mathbf{i}\ell}{2}\sqrt{3} \,\middle|\, k, \ell \in \mathbb{Z},\ k + \ell \in 2\mathbb{Z}\right\}. \tag{2}$$

The elements of Λ form the vertices of a triangulation of the complex plane by equilateral triangles of sidelength 1. Define the map $N : \Lambda \to \mathbb{Z}$ by

$$\Lambda(x) := |x|_{\mathbb{C}}^2 = u^2 + v^2 - uv$$

for $x = u + v\omega \in \Lambda$ with $u, v \in \mathbb{Z}$. Then $N(x) \geq 0$ and

$$N(1) = 1, \qquad N(xy) = N(x)N(y) \tag{3}$$

for all $x, y \in \Lambda$. An element $x \in \Lambda$ is called a **unit** iff $x \neq 0$ and $x^{-1} \in \Lambda$. Thus $x \in \Lambda$ is a unit if and only if $N(x) = 1$ or, equivalently, x is a sixth root of unity. An element $p \in \Lambda$ with $N(p) > 1$ is called a **prime** iff every pair $x, y \in \Lambda$ with $xyp^{-1} \in \Lambda$ satisfies $xp^{-1} \in \Lambda$ or $yp^{-1} \in \Lambda$. It is called **irreducible** iff, for every pair $x, y \in \Lambda$ satisfying $xy = p$, one of the elements x or y is a unit. Evidently, every prime is irreducible.

Lemma 1. Λ *is a principal ideal domain.*

Proof. Let $\mathcal{J} \subset \Lambda$ be a nonzero ideal and choose $x \in \mathcal{J} \setminus \{0\}$ such that

$$N(x) = \min \left\{ N(y) \,\middle|\, y \in \mathcal{J},\, y \neq 0 \right\}. \tag{4}$$

Fix an element $y \in \mathcal{J}$. Then the geometry of the set $\Lambda \subset \mathbb{C}$ shows that every element of the complex plane is contained in an equilateral triangle with sidelength 1, whose vertices belong to the set Λ. Hence every point in the complex plane has a distance at most $1/\sqrt{3}$ to some element of Λ. Thus there exists an element $t \in \Lambda$ such that $|t - y/x| \leq 1/\sqrt{3}$. This implies

$$N(xt - y) = |xt - y|^2 = |t - y/x|^2 \, |x|^2 \leq \frac{1}{3} |x|^2 < |x|^2 = N(x).$$

Since $xt - y \in \mathcal{J}$, it follows from (4) that $xt - y = 0$. Thus we have shown that $\mathcal{J} = \{xt \,|\, t \in \Lambda\}$ is a principal ideal and this proves Lemma 1. □

Lemma 2. *Let $p \in \Lambda$ be a nonzero element which is not a unit. Then p is irreducible if and only if p is a prime.*

Proof. Assume that p is irreducible. We prove that the set

$$\mathcal{J} := \langle p \rangle = \left\{ ps \,\middle|\, s \in \Lambda \right\} = \left\{ \lambda \in \Lambda \,\middle|\, \lambda p^{-1} \in \Lambda \right\}$$

is a maximal ideal in Λ. To see this, note first that $1 \notin \mathcal{J}$ and so $\mathcal{J} \neq \Lambda$. Now let $\mathcal{J}' \subset \Lambda$ be any ideal such that $\mathcal{J} \subsetneq \mathcal{J}'$. Then, by Lemma 1, there exists an element $x \in \Lambda$ such that $\mathcal{J}' = \langle x \rangle$. Since $p \in \mathcal{J} \subset \mathcal{J}'$, this implies that there exists an element $y \in \Lambda$ such that $p = xy$. Since p is irreducible, it follows that x or y is a unit. If y is a unit, we find that $\mathcal{J}' = \langle x \rangle = \langle p \rangle = \mathcal{J}$, in contradiction to our assumption. Hence y is not a unit, hence x is a unit, and hence $\mathcal{J}' = \langle x \rangle = \Lambda$. Thus $\mathcal{J}$ is a maximal ideal as claimed.

We prove that p is a prime. Let $x, y \in \Lambda$ such that $xyp^{-1} \in \Lambda$ and suppose that $xp^{-1} \notin \Lambda$. Then $xy \in \mathcal{J}$ and $x \notin \mathcal{J}$. Hence the set

$$\mathcal{J}' := \{ps + xt \,|\, s, t \in \Lambda\}$$

is an ideal in Λ which properly contains $\mathcal{J}$. Since $\mathcal{J}$ is maximal, it follows that $\mathcal{J}' = \Lambda$ and so $1 \in \mathcal{J}'$. Thus there exist $s, t \in \Lambda$ such that $ps + xt = 1$ and hence $yp^{-1} = (ps+xt)yp^{-1} = sy + txyp^{-1} \in \Lambda$. This proves Lemma 2. □

Lemma 2 is a general result about principal ideal domains. It shows that every nonzero element of Λ which is not a unit can be expressed as a product of primes, and that this factorization is unique up to reordering and multiplication of each prime factor by a unit.

2 Cubes and squares

Lemma 3. *Let u and v be nonzero integers and assume that they are coprime. Then the following are equivalent.*

(i) *There exists an integer $s \in \mathbb{Z}$ such that*

$$u^2 + 3v^2 = s^3. \tag{5}$$

(ii) *There exist integers $a, b \in \mathbb{Z}$ such that*

$$u = a\big(a^2 - 9b^2\big), \qquad v = 3b\big(a^2 - b^2\big). \tag{6}$$

Proof. We prove that (ii) implies (i). Assume $a, b \in \mathbb{Z}$ satisfy (6). Then

$$\begin{aligned} u^2 + 3v^2 &= a^2\big(a^4 - 18a^2b^2 + 81b^4\big) + 27b^2\big(a^4 - 2a^2b^2 + b^4\big) \\ &= a^6 + 9a^4b^2 + 27a^2b^4 + 27b^6 \\ &= (a^2 + 3b^2)^3. \end{aligned}$$

Thus we have proved that (ii) implies (i) with $s := a^2 + 3b^2$.

We prove that (i) implies (ii). Let s be an integer satisfying (5). We prove in eight steps that there exist integers a, b that satisfy (6).

Step 1. *u and v have opposite parity.*

Since u, v are coprime, they cannot both be even. Suppose, by contradiction, that u and v are both odd and define $k := (u-1)/2$ and $\ell := (v-1)/2$. Then k and ℓ are integers and $2k + 1 = u$ and $2\ell + 1 = v$. Hence

$$u^2 + 3v^2 = 4k^2 + 4k + 1 + 12\ell^2 + 12\ell + 3 = 8m + 4,$$

where $m := k(k+1)/2 + 3\ell(\ell+1)/2 \in \mathbb{Z}$. Thus $u^2 + 3v^2$ is an even number which is not divisible by 8 and hence cannot be cube, in contradiction to our assumption in (i). This proves Step 1.

Step 2. *u is not divisible by* 3.

Suppose, by contradiction, that $u = 3k$ for some integer k. Then, by our coprime assumption, v is not divisible by 3. Hence there exist integers $\ell \in \mathbb{Z}$ and $\varepsilon \in \{+1, -1\}$ such that $v = 3\ell + \varepsilon$. This implies

$$u^2 + 3v^2 = 9k^2 + 3\big(9\ell^2 + 6\ell\varepsilon + 1\big) = 9m + 3,$$

where $m := k^2 + 3\ell^2 + 2\ell\varepsilon \in \mathbb{Z}$. Since the cube of any integer is congruent to ± 1 modulo 9, this contradicts our assumption in (i) and proves Step 2.

Step 3. *The integers u^2+3v^2 and $2u$ are coprime.*

By Step 1, u and v have opposite parity and so u^2+3v^2 is odd. Moreover, by Step 2 the number u is not divisible by 3. Thus, if $p \in \mathbb{N}$ is a prime that divides $2u$, then $p \notin \{2,3\}$, hence p divides u, hence p does not divide v, and hence p does not divide u^2+3v^2. This proves Step 3.

Step 4. *Let k and ℓ be coprime nonzero integers. Then k and ℓ are coprime in the ring Λ of Eisenstein integers in (2).*

Let $x \in \Lambda \setminus \{0\}$ such that $kx^{-1} \in \Lambda$ and $\ell x^{-1} \in \Lambda$. Then

$$\frac{k^2}{N(x)} = N(kx^{-1}) \in \mathbb{Z}, \qquad \frac{\ell^2}{N(x)} = N(\ell x^{-1}) \in \mathbb{Z}.$$

Since k and ℓ are coprime, so are k^2 and ℓ^2. Hence $N(x)=1$ and hence x is a unit in Λ. This proves Step 4.

Step 5. *The elements $u+v+2v\omega$ and $u-v-2v\omega$ are coprime in Λ.*

Let $x \in \Lambda \setminus \{0\}$ such that

$$\frac{u+v+2v\omega}{x} \in \Lambda, \qquad \frac{u-v-2v\omega}{x} \in \Lambda.$$

Then, since $1+2\omega = \mathbf{i}\sqrt{3}$, we find that

$$\begin{aligned}\frac{u^2+3v^2}{x} &= \frac{u+v+2v\omega}{x} \cdot \bigl(u-v-2v\omega\bigr) \in \Lambda,\\ \frac{2u}{x} &= \frac{u+v+2v\omega}{x} + \frac{u-v-2v\omega}{x} \in \Lambda.\end{aligned}$$

Since u^2+3v^2 and $2u$ are coprime by Step 3, it follows from Step 4 that x is a unit in Λ. This proves Step 5.

Step 6. *There exist elements $x, \varepsilon \in \Lambda$ such that*

$$u+v+2v\omega = x^3\varepsilon, \qquad N(\varepsilon)=1. \tag{7}$$

By assumption in part (i) we have

$$\bigl(u+v+2v\omega\bigr)\cdot\bigl(u-v-3v\omega\bigr) = u^2+3v^2 = s^3.$$

By the unique factorization property of the ring Λ of Eisenstein integers (Lemma 2), the number s is a product of primes $p_1,\dots,p_n$ in Λ. By Step 5, each factor p_i divides either $u+v+2v\omega$ or $u-v-2v\omega$, but not both. Define $I := \{i \,|\, (u+v+2v\omega)p_i^{-1} \in \Lambda\}$ and $x := \prod_{i\in I} p_i$ and $y := s/x$. Then $\varepsilon := (u+v+2v\omega)x^{-3} \in \Lambda$ and $\delta := (u-v-2v\omega)y^{-3} \in \Lambda$ and $\delta\varepsilon = 1$. Hence ε is a unit in Λ and this proves Step 6.

Step 7. *There exist $a, b \in \mathbb{Z}$ and $\theta \in \Lambda$ such that*

$$u + \mathbf{i}v\sqrt{3} = \left(a + \mathbf{i}b\sqrt{3}\right)^3 \theta, \qquad N(\theta) = 1. \tag{8}$$

By Step 6 there exist $k, \ell \in \mathbb{Z}$ and $\varepsilon \in \Lambda$ such that

$$u + \mathbf{i}v\sqrt{3} = u + v + 2v\omega = (k + \ell\omega)^3 \varepsilon, \qquad N(\varepsilon) = 1. \tag{9}$$

If ℓ is even, then (8) holds with $a := k - \ell/2$, $b := \ell/2$, and $\theta = \varepsilon$. Thus assume that ℓ is odd and choose $r, s \in \{+1, -1\}$ such that

$$2k - \ell - r \in 4\mathbb{Z}, \qquad \ell - s \in 4\mathbb{Z}. \tag{10}$$

Define

$$\eta := \frac{r}{2} + \frac{\mathbf{i}s}{2}\sqrt{3}. \qquad a := \frac{(2k - \ell)r + 3\ell s}{4}, \qquad b := \frac{\ell r - (2k - \ell)s}{4}. \tag{11}$$

Then η is a unit in Λ and, by (10), a and b are integers. Moreover,

$$\begin{aligned} (k + \ell\omega)\overline{\eta} &= \left(\frac{2k - \ell}{2} + \frac{\mathbf{i}\ell}{2}\sqrt{3}\right)\left(\frac{r}{2} - \frac{\mathbf{i}s}{2}\sqrt{3}\right) \\ &= \frac{(2k - \ell)r + 3\ell s}{4} + \mathbf{i}\frac{\ell r - (2k - \ell)s}{4}\sqrt{3} = a + \mathbf{i}b\sqrt{3}. \end{aligned}$$

Thus (8) holds with $\theta = \eta^3 \varepsilon$. This proves Step 7.

Step 8. *There exist integers $a, b \in \mathbb{Z}$ such that*

$$u + \mathbf{i}v\sqrt{3} = \left(a + \mathbf{i}b\sqrt{3}\right)^3. \tag{12}$$

Moreover, equation (12) *is equivalent to* (6)*.*

We prove that the unit $\theta \in \Lambda$ in Step 7 is real. Suppose, by contradiction, that this is not the case. Then there exist integers $r, s \in \{+1, -1\}$ such that $\theta = \frac{1}{2}(r + \mathbf{i}s\sqrt{3})$. Hence it follows from (8) that

$$u + \mathbf{i}v\sqrt{3} = \left(a + \mathbf{i}b\sqrt{3}\right)^3 \theta = \left(a\left(a^2 - 9b^2\right) + 3b\left(a^2 - b^2\right)\mathbf{i}\sqrt{3}\right)\theta. \tag{13}$$

Thus

$$u = \frac{r}{2}a\left(a^2 - 9b^2\right) - \frac{s}{2}9b\left(a^2 - b^2\right), \qquad v = \frac{s}{2}a\left(a^2 - 9b^2\right) + \frac{r}{2}3b\left(a^2 - b^2\right).$$

Since u and v are integers, it follows that a and b have the same parity, and hence u and v are both even, in contradiction to Step 1. Thus $\theta \in \{+1, -1\}$ as claimed. By changing the signs of a and b, if necessary, we may assume that $\theta = 1$. Hence (12) holds. Moreover, the equivalence of (6) and (12) follows from (13) with $\theta = 1$. This proves Step 8 and Lemma 3. □

3 Euler's proof of FLT for the exponent 3

Theorem 4 (**FLT for** $n = 3$)**.** *The equation*

$$x^3 + y^3 + z^3 = 0 \tag{14}$$

does not admit a solution $x, y, z \in \mathbb{Z}$ *such that* $xyz \neq 0$*.*

Proof. The proof is by *infinite descent*. It is based on the observation that every nonempty set of positive integers contains a smallest element. The proof will show that the set

$$\mathscr{F} := \left\{ |xyz| \,\middle|\, x, y, z \in \mathbb{Z},\, x^3 + y^3 + z^3 = 0,\, xyz \neq 0 \right\} \tag{15}$$

cannot contain any smallest element and hence must be empty. Suppose, by contradiction, that the set $\mathscr{F}$ is nonempty and choose a triple of nonzero integers x, y, z such that (14) holds and

$$|xyz| = \min \mathscr{F}. \tag{16}$$

We prove in eight steps that there exist nonzero integers k, ℓ, m such that

$$k^3 + \ell^3 + m^3 = 0, \qquad 0 < |k\ell m| < |xyz|, \tag{17}$$

in contradiction to (16). This contradiction shows that the set $\mathscr{F}$ is empty.

Step 1. *The numbers* x, y, z *are pairwise coprime.*

If there exists a prime p that divides two of the number x, y, z, then p divides all three numbers, and hence

$$x' := x/p, \qquad y' := y/p, \qquad z' := z/p$$

are integers satisfying (14) and $0 < |x'y'z'| < |xyz|$ in contradiction to (16). This proves Step 1.

Step 2. *Precisely one of the numbers* x, y, z *is even.*

If two of the numbers x, y, z are even, so is the third, in contradiction to Step 1. Hence at most one of the numbers x, y, z is even, and so at least two of the numbers x, y, z are odd. But if two of these numbers are odd, then the third one is necessarily even. This proves Step 2.

Standing assumption. *We assume from now on, without loss of generality, that z is even and hence the numbers x and y are odd.*

Step 3. *Define the numbers u, v by*

$$u := \frac{x+y}{2}, \qquad v := \frac{x-y}{2}. \tag{18}$$

Then u and v are coprime nonzero integers, have opposite parity, and satisfy

$$2u(u^2+3v^2)+z^3=0. \tag{19}$$

If $x=-y$, then (14) implies $z=0$ and. if $x=y$, then (14) implies $z^3=-2x^3$ and so x is even, in contradiction to our standing assumption. Thus u and v are nonzero integers. They satisfy

$$u+v=x, \qquad u-v=y$$

and hence have opposite parity, because x and y are odd. Moreover, u and v are coprime, because x and y are coprime. By (14) the numbers u and v also satisfy $-z^3=(u+v)^3+(u-v)^3=2u^3+6uv^2=2u(u^2+3v^2)$. This proves (19) and Step 3.

Step 4. *u is even and v is odd.*

By Step 3 the numbers u and v have opposite parity and hence u^2+3v^2 is odd. Moreover, since z is even, the number $-z^3$ is divisible by 8. Hence, by equation (19), $2u$ is divisible by 8, and so u is divisible by 4. Since u and v have opposite parity, it follows that v us odd, and this proves Step 4.

Step 5. *If $u \notin 3\mathbb{Z}$, then the numbers $2u$ and u^2+3v^2 are coprime.*

Assume that u is not divisible by 3 and, by contradiction, that p is a common prime divisor of $2u$ and u^2+3v^2. Then $p \notin \{2,3\}$ because u^2+3v^2 is odd. Hence p divides u, hence p divides $3v^2$, hence p divides v^2, and hence p a common divisor of u and v, in contradiction to Step 3. This proves Step 5.

Step 6. *If $u \in 3\mathbb{Z}$, then the numbers $6u$ and $u^2/3+v^2$ are coprime.*

By Step 3 v is not divisible by 3 and, by Step 4, $u/3$ is even and v is odd. Hence the number $u^2/3+v^2=3(u/3)^2+v^2$ is odd and is not divisible by 3. Suppose, by contradiction, that there exists a common prime divisor p of $6u$ and $u^2/3+v^2$. Then $p \notin \{2,3\}$, hence p divides $u/3$, and hence p is a common divisor of u and v, in contradiction to Step 3. This proves Step 6.

Step 7. *If $u \notin 3\mathbb{Z}$, then there exist integers k, ℓ, m satisfying* (17).

Assume that u is not divisible by 3. Then $2u$ and $u^2 + 3v^2$ are coprime by Step 5. Thus, by equation (19) in Step 3, there exist integers r, s such that

$$2u = r^3, \qquad u^2 + 3v^2 = s^3. \tag{20}$$

Hence, by Lemma 3 there exist integers a, b such that

$$u = a(a^2 - 9b^2), \qquad v = 3b(a^2 - b^2). \tag{21}$$

Since u and v are nonzero, so are the numbers $a, b, a-3b, a+3b, a-b, a+b$. Moreover, it follows from (20) and (21) that

$$r^3 = 2u = 2a(a-3b)(a+3b). \tag{22}$$

We prove that the numbers $2a$, $a-3b$, and $a+3b$ are pairwise coprime. To see this, note first that by (21) and Step 3 the numbers a and b are coprime and that they have opposite parity, because otherwise v would be even, in contradiction to Step 4. Thus $a^2 - 9b^2$ and $a^2 - b^2$ are odd and so a is even and b is odd, again by Step 4. Moreover, a is not divisible by 3, because u is not devisible by 3. Thus $a - 3b$ is odd and is not devisible by 3. Hence any common prime divisor of $2a$ and $a - 3b$ cannot be equal to 2 or 3, and therefore must also be a prime divisor of a and b, in contradiction to the fact that a and b are coprime. This shows that $2a$ and $a - 3b$ are coprime. Since $2a = (a+3b) + (a-3b)$, it follows that also $2a$ and $a+3b$ are coprime, as are $a+3b$ and $a-3b$.

Since the numbers $2a$, $a-3b$, and $a+3b$ are nonzero and pairwise coprime, it follows from (22) that there exist nonzero integers k, ℓ, m such that

$$k^3 = -2a, \qquad \ell^3 = a - 3b, \qquad m^2 = a + 3b.$$

Take the sum of these equations to obtain

$$k^3 + \ell^3 + m^3 = 0$$

and take the product to obtain

$$\begin{aligned} |k\ell m|^3 &= |2a(a^2 - 9b^2)| = |2u| \\ &= |x+y| \le |x| + |y| < 2\,|x|\,|y| \le |xyz|\,. \end{aligned}$$

Thus k, ℓ, m satisfy (17) and this proves Step 7.

Step 8. *If $u \in 3\mathbb{Z}$, then there exist integers k, ℓ, m satisfying* (17)*.*

Assume $u \in 3\mathbb{Z}$ and define $w := u/3$. Then $w \in \mathbb{Z}$ and, by (19), we have

$$-z^3 = 2u\big(u^2 + 3v^2\big) = 6w\big(9w^2 + 3v^2\big) = 18w\big(v^2 + 3w^2\big).$$

By Step 3 the numbers v and w are coprime, by Step 4 the number w is even and v is odd, and by Step 6, the numbers $18w$ and $v^2 + 3w^2$ are coprime. Hence there exist integers r, s such that

$$18w = r^3, \qquad v^2 + 3w^2 = s^3. \tag{23}$$

Since v, w are coprime, it follows from Lemma 3 and equation (23) that there exist integers a, b such that

$$v = a\big(a^2 - 9b^2\big), \qquad w = 3b\big(a^2 - b^2\big). \tag{24}$$

Since v and w are nonzero, so are the numbers $a, b, a - 3b, a + 3b, a - b, a + b$. Since v, w are coprime and w is even, it follows that a, b are coprime and have opposite parity. Thus a is odd and b is even. Also, by (23) and (24),

$$r^3 = 18w = 54b(a - b)(a + b).$$

Hence r is divisible by 3 and

$$\left(\frac{r}{3}\right)^3 = 2b(a - b)(a + b).$$

Since a, b are coprime, a is odd, and b is even, the numbers $2b, a - b, a + b$ are pairwise coprime. Hence there exist nonzero integers k, ℓ, m such that

$$k^3 = -2b, \qquad \ell^3 = b - a, \qquad m^3 = b + a.$$

Take the sum of these identities to obtain

$$k^3 + \ell^3 + m^3 = 0,$$

and take their product to obtain

$$\begin{aligned} |k\ell m|^3 &= \big|2b(a^2 - b^2)\big| = \frac{|r^3|}{27} = \frac{|18w|}{27} = \frac{|2u|}{9} \\ &= \frac{|x + y|}{9} < |x + y| \le |x| + |y| < 2\,|x|\,|y| \le |xyz|\,. \end{aligned}$$

Thus k, ℓ, m satisfy (17) and this proves Step 8.

By Step 7 and Step 8 the set $\mathscr{F} \subset \mathbb{N}$ in (15) does not contain any minimal element and hence must be empty. This proves Theorem 4. □

There is no claim to originality in these notes. The purpose is merely to translate and spell out in slightly more detail the beautiful exposition by Günter Bergmann [1] of the proof of Fermat's Last Theorem for the exponent three given by Leonhard Euler in 1770. In particular, the proof of Lemma 3 in these notes follows closely the exposition in [1].

References

[1] Günter Bergmann, Über Eulers Beweis des großen Fermatschen Satzes für den Exponenten 3. *Mathematische Annalen* **164** (1966), 159–175. `https://gdz.sub.uni-goettingen.de/id/PPN235181684_0164?tify`