Fermat's Last Theorem:

We have completely classified the integer solutions to the equation

$$x^2+y^2=z^2$$

when studying congruent numbers. The natural question is what about

$$x^3+y^3=z^3$$

or more generally

$$x^n+y^n=z^n$$

for $n>2$. Fermat asserted that he could prove there were no solutions $x,y,z \in \mathbb{Z}$ w/ $xyz \neq 0$. This became known as Fermat's Last Theorem. It remained unproved until ~~the~~ 1995 when a proof was finally given by Andrew Wiles. This is a very difficult proof and actually uses elliptic curves! What we are going to do is prove the result for the rather easy cases of $n=3$ and $n=4$. It turns out that $n=4$ is much easier than $n=3$ so we begin here. Fermat actually gave a proof in this case via his method of descent. What he actually proved is there are no nontrivial integer solutions to $x^4+y^4=z^2$, which immediately implies the result since we can write

$$x^4 + y^4 = z^4$$
$$= (z^2)^2.$$

Thm: The equation $x^4+y^4=z^2$ has no solution in positive integers.

Proof: Consider $x, y, z \in \mathbb{Z}_{>0}$ s.t.

$$x^4+y^4=z^2 \qquad (*).$$

Let $d=\gcd(x,y)$. Then $d^4 \mid (x^4+y^4) \Rightarrow d^4 \mid z^2$ $\Rightarrow d^2 \mid z$. Write $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$, $z_1 = \frac{z}{d^2}$. Then

$$x_1^4 + y_1^4 = z_1^2$$

and $\gcd(x_1, y_1) = 1$. This gives that x_1^2, y_1^2, z_1 is a primitive Pythagorean triple. Thus $\exists\, m, n \in \mathbb{Z}_{>0}$ s.t.

$$x_1^2 = 2mn$$
$$y_1^2 = m^2 - n^2$$
$$z_1 = m^2 + n^2.$$

Recall that we showed before that y_1^2 is necessarily odd. This implies that m and n are of opposite parity, i.e., one is odd and one is even. We need to determine which is which. We have

$$y_1^2 + n^2 = m^2$$

is a primitive Pythagorean triple and y_1 is odd, so we must have n even and m odd.

Set $u = m$ and $v = 2n$. Since n is even, we can write $n = 2n'$. We have that

$$uv = x_1^2.$$

and $\gcd(u,v) = 1$. Thus we have that u and v must each be a perfect square. (Let $p \mid x_1$. Then $p^2 \mid uv$ and since $\gcd(u,v) = 1$, $p^2 \mid u$ or $p^2 \mid v$. This splits the primes dividing x_1^2 up ... continue this..)

So $\exists\ a, b$ s.t. $u = a^2$ and $v = b^2$. Thus, $m = a^2$ and $2n = b^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$. Thus, $2n = 4B^2$ $\Rightarrow n = 2c^2$. for $2c = b$. Now observe we have

$$a^4 = m^2 = y_1^2 + n^2$$

$$= y_1^2 + 4c^4.$$

Thus, a solution of $x^4 + y^4 = z^2$ leads to a solution of the equation

$$a^4 = y^2 + 4c^4. \quad (**)$$

Moreover,

$$a \le a^4 = m^2 < m^2 + n^2 = z_1 \le z.$$

Thus we obtain a solution of (**) with $a < z$.

We will now show a solution of (**) leads to a solution of (*) w/ $z_2 \le a$. This will give a contradiction as we will then have a strictly decreasing sequence of positive integers.

Let (a, b, c) be such that (pos. integers)

$$a^4 = b^2 + 4c^4. \qquad (**')$$

Set $e = \gcd(a, c)$. Then $e^4 \mid b^2 \Rightarrow e^2 \mid b$. Consider $a_1 = \frac{a}{e}$, $b_1 = \frac{b}{e^2}$, $c_1 = \frac{c}{e}$. We have that a_1, b_1, c_1 satisfy (**') with $\gcd(a_1, c_1) = 1$. Thus, we have

$$(a_1^2)^2 = b_1^2 + (2c_1^2)^2$$

and so a_1^2, b_1, $2c_1^2$ are a primitive Pythagorean triple. So $\exists\ m', n'$ s.t.

$$2c_1^2 = 2m'n' \Rightarrow c_1^2 = m'n'.$$

$$b_1 = (m')^2 - (n')^2$$

$$a_1^2 = (m')^2 + (n')^2.$$

Using that

$$c_1^2 = m'n'$$

and that $\gcd(m', n') = 1$, we see that m' and n' must be perfect squares. i.e, $\exists\ x_2, y_2$ s.t.

$$m' = x_2^2$$
$$n' = y_2^2.$$

Let $z_2 = a_1$ we have

$$x_2^4 + y_2^4 = (m')^2 + (n')^2$$
$$= a_1^2 = z_2^2$$

and so (x_2, y_2, z_2) is a positive solution to $(*)$.

Moreover, $z_2 = a_1 \leq a$.

Hence $z_2 < z_1$. We can now apply the same process to z_2 to get z_3 w/

$$z_3 < z_2 < z_1.$$

This process can be repeated forever. However, these are all positive integers. #. Thus there can be no solution to $(*)$ to begin with.

∎

Though the proof of this theorem was tedious, it did not really require anything more than prime numbers, Pythagorean triples and being clever. The proof for exponent 3 requires more machinery, which we now begin to set up.

Def: A complex number ξ is an <u>algebraic integer</u> (or is <u>integral</u>) if $\exists$ a monic polynomial $f(x)$ with integer coefficients so that

$$f(\xi) = \xi^n + a_1 \xi^{n-1} + \dots + a_n = 0$$

w/ $a_i \in \mathbb{Z}$.

Example: ① $\sqrt{2}$ is an algebraic integer:

$$f(x) = x^2 - 2$$

satisfies $f(\sqrt{2}) = 0$.

② i is an algebraic integer.

$$f(x) = x^2 + 1$$

satisfies $f(i) = 0$

③ $\sqrt[n]{a}$ is an algebraic integer:

$$f(x) = x^n - a$$

satisfies $f(\sqrt[n]{a}) = 0$.

The reason they are called algebraic integers is they generalize the notion of integers to larger sets. (fields)

Thm: All integers are algebraic integers. The only algebraic integers in $\mathbb{Q}$ are those elements in $\mathbb{Z}$.

Proof: Let $m \in \mathbb{Z}$. Then clearly m is an algebraic integer as $f(x) = x - m$ has integer coefficients and satisfies $f(m) = 0$.

Now suppose $\frac{b}{c} \in \mathbb{Q}$ is an algebraic integer. Then $\exists$ $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ w/ $a_i \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, (The n can be different for different algebraic integers of course!) with $f(\frac{b}{c}) = 0$. We may assume $\frac{b}{c}$ is in lowest terms so that $\gcd(b,c) = 1$. Then

$$\left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_1\left(\frac{b}{c}\right) + a_0 = 0.$$

Multiply both sides by c^n:

$$b^n + a_{n-1}c\,b^{n-1} + \cdots + a_1 c^{n-1} b + c^n a_0 = 0$$

$$\Rightarrow b^n = c\left(-a_{n-1}b^{n-1} - \cdots - a_1 c^{n-2} b + c^{n-1} a_0\right)$$

$$\Rightarrow c \mid b^n \Rightarrow c = \pm 1.$$ Thus, $\frac{b}{c} \in \mathbb{Z}$. ∎

In general, given a set $K \subseteq \mathbb{C}$ we write $\mathcal{O}_K$ for the set of algebraic integers in K. (Normally we take K to be a finite field of $\mathbb{Q}$ and then $\mathcal{O}_K$ is a ring!)

Thus $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

We will mainly be interested in the sets

$$K = \mathbb{Q}(\sqrt{m}) = \{ a + b\sqrt{m} : a, b \in \mathbb{Q} \}.$$

for $m \in \mathbb{Z}$.

Def: The minimal polynomial of an algebraic integer ξ is the polynomial $g(x) \in \mathbb{Q}[x]$ of smallest degree so that $g(\xi) = 0$.

Thm: The minimal polynomial of an algebraic integer is monic with integer coefficients.

This theorem is not difficult to prove, but would require us to talk about polynomials more which we don't really have time to do.

Def: Let $\alpha \in \mathbb{Q}(\sqrt{m})$ w/ $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$. We define the norm of α by

$$N(\alpha) = \alpha\bar{\alpha}$$

where $\bar{\alpha} = a - b\sqrt{m}$ is the conjugate of α. ($\sqrt{m} \notin \mathbb{Q}$ here!)

Note: $N(\alpha) = a^2 - b^2 m$.

Def: Let α and β be algebraic integers. We say $\alpha | \beta$ if there exists an algebraic integer γ s.t. $\alpha\gamma = \beta$. We say α is a <u>unit</u> if $\alpha | 1$, i.e if $\exists$ an algebraic integer γ s.t $\alpha\gamma = 1$.

Thm: ① $N(\alpha\beta) = N(\alpha)N(\beta)$

② $N(\alpha) = 0$ iff $\alpha = 0$

③ If α is an algebraic integer, then $N(\alpha) \in \mathbb{Z}$.

④ If α is an algebraic integer, then $N(\alpha) = \pm 1$ iff α is a unit.

Proof: ① Exercise. This is just a calculation, compare each side.

② If $\alpha = 0$ it is clear $N(\alpha) = 0$. Now suppose $N(\alpha) = 0$, i.e, if $\alpha = a + b\sqrt{m}$, then $a^2 - b^2 m = 0$ If $b \neq 0$, then $m = \left(\frac{a}{b}\right)^2 \Rightarrow \sqrt{m} \in \mathbb{Q}$. $\#$. Thus $b = 0 \Rightarrow a = 0$.

③ Let $f(x)$ be the minimal polynomial of α. If $\deg f(x) = 1$, then $f(x) = x - \alpha \Rightarrow \alpha \in \mathbb{Z} \Rightarrow N(\alpha) = \alpha^2 \in \mathbb{Z}$.

Suppose $\deg f(x) > 1$ so that $\alpha \notin \mathbb{Z}$. Then we have

$\alpha = a + b\sqrt{m} \Rightarrow$

$$x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = 0 \quad \text{when } x = \alpha$$

Since this is degree 2 and $\deg f(x) > 1$, we must have this is $f(x)$. Our earlier theorem said this has integer coefficients, so $\alpha\bar{\alpha} \in \mathbb{Z}$, i.e $N(\alpha) \in \mathbb{Z}$.

④ Suppose $N(\alpha) = \pm 1$. Then $\alpha\bar{\alpha} = \pm 1 \Rightarrow \alpha | 1 \Rightarrow \alpha$ is a unit.

Suppose $\alpha | 1$. Then $\exists \gamma$ an alg. integer s.t $\alpha\gamma = 1 \Rightarrow$

$N(\alpha)N(\gamma) = N(\alpha\gamma) = \pm 1$. Thus $N(\alpha) \mid \pm 1$ and since $N(\alpha) \in \mathbb{Z}$

we must have $N(\alpha) = \pm 1$. ∎

Thm: Let $K = \mathbb{Q}(\sqrt{-3})$. Then

$$\mathcal{O}_K = \mathbb{Z}\left[\tfrac{1+\sqrt{-3}}{2}\right] = \left\{ a + b\left(\tfrac{1+\sqrt{-3}}{2}\right) : a, b \in \mathbb{Z} \right\}.$$

Proof: A statement similar to this is true in general, but we are only interested in $\mathbb{Q}(\sqrt{-3})$ so we stick to that case. First we show elements of the form $a + b\left(\frac{1+\sqrt{-3}}{2}\right)$ are actually algebraic. Let $\alpha = a + b\left(\frac{1+\sqrt{-3}}{2}\right)$. Observe that $\bar{\alpha} = a + b\left(\frac{1-\sqrt{-3}}{2}\right)$ and that we have

$$f(\alpha) = 0$$

for $f(x) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$. Our goal is to show $\alpha + \bar{\alpha}$ and $\alpha\bar{\alpha}$ are integers.

$$\alpha + \bar{\alpha} = 2a + b \in \mathbb{Z}$$

$$\alpha\bar{\alpha} = \left(a + \frac{b}{2}\right)^2 + \frac{3b^2}{4}$$

$$= a^2 + b + b^2 \in \mathbb{Z}.$$

Thus, α is the zero of a monic poly w/ integer coefficients so α is an algebraic integer. Now we must show these are all the algebraic integers.

Let $\alpha = \dfrac{a+b\sqrt{-3}}{c} \in \mathbb{Q}(\sqrt{-3})$ w/ $\gcd(a,b,c)=1$. We can write any element in this form. (exercise!) Suppose α is an algebraic integer. Then we must have

$$f(x) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha}$$

has coefficients in $\mathbb{Z}$ since $f(\alpha)=0$ and no poly of lower degree has α as a zero. So our earlier theorem gives it has coefficients in $\mathbb{Z}$. Thus, $\alpha+\bar{\alpha} = \frac{2a}{c} \in \mathbb{Z}$ and $c^2 \mid a^2+3b^2$ since $\frac{a^2+3b^2}{c^2} = \alpha\bar{\alpha}$. If $c=1$, then we have $\alpha = a + b\sqrt{-3}$ which we can write as $(a-b) + 2b\left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Suppose now that $c>1$.

If $c \neq 2$, then we must have $\gcd(a,c)>1$ since $\frac{2a}{c} \in \mathbb{Z}$ so $c \mid 2a$. Let p be a prime w/ $p \mid a$ and $p \mid c$. Then we use that $c^2 \mid a^2+3b^2$ to get $n \in \mathbb{Z}$ s.t. $nc^2 = a^2+3b^2$. But then $p^2 \mid 3b^2 \Rightarrow p \mid b$ # since $\gcd(a,b,c)=1$.

So we must have $c=2$. Thus, $a^2+3b^2 \equiv 0 \pmod 4$ $\Rightarrow$ a and b are both odd or even. They can't both be even because then $\gcd(a,b,c) \geq 2$. Thus a and b are both odd.

Thus, $\dfrac{a+b\sqrt{-3}}{2} = \dfrac{a-b}{2} + b\left(\dfrac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

since $\frac{a-b}{2} \in \mathbb{Z}$ because a and b both odd. Thus we have the result.

Theorem: The units in $\mathbb{Q}(\sqrt{-3})$ are exactly the elements

$$\pm 1, \quad \frac{1 \pm \sqrt{-3}}{2}, \quad \frac{-1 \pm \sqrt{-3}}{2}.$$

Proof: We need to determine the algebraic integers that are have norm ± 1. First, observe that for $a + b\sqrt{-3}$ w/ $a, b \in \mathbb{Z}$, $N(a+b\sqrt{-3}) = a^2+3b^2 \geq 0$. So we can never have norm -1 in this case. We only have norm 1 when $a = \pm 1, b = 0$. So ± 1 are units.

Consider now $\frac{a+b\sqrt{-3}}{2} \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ w/ a, b, odd. Then $N\left(\frac{a+b\sqrt{-3}}{2}\right) = \frac{a^2+3b^2}{4} = \pm 1$. Again, this is always greater than or equal to 0, so we really want to study

$$\frac{a^2+3b^2}{4} = 1.$$

i.e.,

$$a^2 + 3b^2 = 4.$$

However, we need a and b odd. If $b > 1$, then $3b^2 > 4$. So $b = \pm 1$. This forces $a = \pm 1$ as well.

This gives the result. ∎

Def: Let $\alpha \in \mathbb{Q}(\sqrt{m})$ be an algebraic integer that is not a unit. We say α is <u>prime</u> if it is divisible only by units and unit times α.

Warning: This generalizes the notion of prime you are used to, with one caveat. Here we allow negatives! So if p is prime, then $-p$ is as well! This is forced on us because there is not a well-defined ordering for $\mathbb{Q}(\sqrt{-m})$, such as in $\mathbb{Q}(\sqrt{-3})$.

Thm: Let $\alpha \in \mathbb{Q}(\sqrt{m})$ and suppose $N(\alpha) = \pm p$ where p is a prime. Then α is necessarily prime.

Proof: Suppose $\alpha = \beta\gamma$. Then $N(\beta)N(\gamma) = \pm p \Rightarrow \cancel{N(\beta) \mid p \text{ or } N(\gamma) \mid p}$ $N(\beta) \mid p \Rightarrow N(\beta) = \pm 1$ or $\pm p$. and $N(\gamma) = \pm p$ or ± 1. Either way, one of them is ± 1 and so β or γ is a unit. $\blacksquare$

Thm: Every algebraic integer in $\mathbb{Q}(\sqrt{m})$ that is not zero or a unit can be factored into a product of primes.

Proof: Let $\alpha \in \mathbb{Q}(\sqrt{m})$ with $\alpha \neq 0$ and α not a unit. If α is prime we are done. If not, write

$$\alpha = \alpha_1 \alpha_2 .$$

If α_1 and α_2 are prime we are done, if not factor them.

Continuing this process we obtain

$$\alpha = \alpha_1 \cdots \alpha_n .$$

If this process does not terminate with primes, then we have n can be arbitrarily large and

$$N(\alpha) = \prod_{i=1}^{n} N(\alpha_i) \Rightarrow |N(\alpha)| = \prod_{i=1}^{n} |N(\alpha_i)| \geq 2^n$$

But this is for any n, a contradiction. ∎

What we are really interested in is not just factorization into primes, rather we want that when an algebraic integer factors into primes it factors uniquely as we had for $\mathbb{Z}$. This is not true in general as you saw in an earlier homework set. Fortunately we do have that $\mathbb{Q}(\sqrt{-3})$ has unique factorization. This takes a couple of steps to prove.

The first step is to show that we can generalize the Euclidean algorithm to this setting. Again, this is not possible for all $\mathbb{Q}(\sqrt{m})$.

<u>Thm:</u> Let α and $\beta \in \mathbb{Q}(\sqrt{-3})$ be algebraic integers w/ $\beta \neq 0$. There exists integers γ and δ of $\mathbb{Q}(\sqrt{-3})$ so that

$$\alpha = \beta\gamma + \delta \quad \text{and } |N(\delta)| < |N(\beta)|.$$

<u>Proof</u>: Let α and β be as in the statement of the theorem.

We have that

$$\frac{\alpha}{\beta} = r + s\sqrt{-3} \quad \text{for } r, s \in \mathbb{Q}.$$

Choose $x \in \mathbb{Z}$ so that x is as close as possible to $2s$. and choose $y \in \mathbb{Z}$ so that $y \equiv x \pmod 2$ and y is as close as possible to $2r$. Then we have

$$|2s - x| \leq 1/2$$

and

$$|2r - y| \leq 1.$$

Since $x \equiv y \pmod 2$, we have that $\gamma = \frac{y + x\sqrt{-3}}{2}$ is an algebraic integer.

Let $\delta = \alpha - \beta\gamma$. One can check using our characterization of the algebraic integers of $\mathbb{Q}(\sqrt{-3})$ as the set $\mathbb{Z}[(\frac{1+\sqrt{-3}}{2})]$ that the product and sum of algebraic integers is again an algebraic integer and so δ is an algebraic integer.

Observe that $\alpha = \beta\gamma + \delta$ by definition and

$$\begin{aligned} N(\delta) &= N(\beta\alpha - \beta\gamma) \\ &= N(\beta)\, N\left(\frac{\alpha}{\beta} - \gamma\right) \\ &= N(\beta)\, N\left(\left(r - \frac{y}{2}\right) + \left(s - \frac{x}{2}\right)\sqrt{-3}\right) \\ &= N(\beta)\left(\left(r - \frac{y}{2}\right)^2 + 3\left(s - \frac{x}{2}\right)^2\right). \end{aligned}$$

Thus,

$$|N(\alpha - \beta\delta)| \leq |N(\beta)|\left(\tfrac{1}{4} + \tfrac{3}{16}\right) < |N(\beta)|$$

since $|2s - x| \leq 1/2 \Rightarrow |s - \frac{x}{2}| \leq \frac{1}{4}$

and $|2r - y| \leq 1 \Rightarrow |r - \frac{y}{2}| \leq \frac{1}{2}$. ▣

We are now able to use this result to show that $\mathbb{Q}(\sqrt{-3})$ has unique factorization.

<u>Thm:</u> Every integer $\alpha \in \mathbb{Q}(\sqrt{-3})$ that is not 0 or a unit can be factored uniquely into primes not taking into account order or multiplication by units.

<u>Proof:</u>

The proof of this theorem essentially follows the same arg. as in the case of $\mathbb{Z}$ now that we have a Euclidean algorithm.

<u>Lemma:</u> Let $\alpha, \beta \in K = \mathbb{Q}(\sqrt{-3})$ be alg. integers having no common factors other than units. Then $\exists\, \gamma, \delta \in \mathcal{O}_K$ s.t.

$$\alpha\gamma + \beta\delta = 1.$$

Proof: Let

$$S = \{ \alpha\gamma + \beta\delta : \gamma, \delta \in \mathcal{O}_K \}.$$

We know that $N(\alpha\gamma + \beta\delta) \in \mathbb{Z}_{\geq 0}$, so we can choose γ_0, δ_0 so that $N(\alpha\gamma_0 + \beta\delta_0)$ is the smallest positive value.

Set $\varepsilon = \alpha\gamma_0 + \beta\delta_0$. We apply the Euclidean alg to α and ε:

$$\alpha = \varepsilon\lambda + \mu \quad , \quad |N(\mu)| < |N(\varepsilon)|.$$

So we have

$$\mu = \alpha - \varepsilon\lambda = \alpha - (\alpha\gamma_0 + \beta\delta_0)\lambda$$
$$= \alpha(1 - \gamma_0\lambda) - \beta\delta_0\lambda.$$

Thus, μ is an alg. integer. However, by the def of ε we see $|N(\mu)| = 0 \Rightarrow \mu = 0$. Thus, $\alpha = \varepsilon\lambda$.

$\Rightarrow \varepsilon \mid \alpha$. Now run the same arg with β and ε to get $\varepsilon \mid \beta$. Thus, we must have ε is a unit, i.e. $\exists\ \varepsilon^{-1}$ w/ $\varepsilon\varepsilon^{-1} = 1$.

So

$$\alpha(\gamma_0\varepsilon^{-1}) + \beta(\delta_0\varepsilon^{-1}) = 1. \quad \blacksquare$$

Lemma: If π is a prime of $\mathbb{Q}(\sqrt{-7})$ and $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

Proof: Suppose $\pi \nmid \alpha$. Then the only common factors shared between π and α can be units (π prime!) $\Rightarrow$ $\exists\ \gamma, \delta \in \mathcal{O}_K$ s.t.

$$\pi\gamma + \alpha\delta = 1.$$

Thus, $\beta = \pi(\gamma\beta) + \alpha(\delta\beta)$.

Since $\pi \mid \alpha\beta$, π divides the RHS $\Rightarrow \pi \mid \beta$. ∎

By induction we extend this to $\pi \mid (\alpha_1 \ldots \alpha_n)$ then $\pi \mid \alpha_i$ for some $1 \leq i \leq n$.

We can now prove that we have unique factorization for $\mathbb{Q}(\sqrt{-3})$.

Proof: Let $\alpha \in \mathcal{O}_K$ w/ $\alpha \neq 0$, unit and let $\alpha = \varpi_1 \ldots \varpi_r = q_1 \ldots q_s$ be two prime factorizations. We have $\varpi_1 \mid q_1 \cdots q_s$ $\Rightarrow \varpi_1 = q_j$ for some j wlog assume $j = 1$. Then $\varpi_2 \ldots \varpi_r = q_2 \ldots q_s$. Continue this process. ∎

We now have the necessary background to prove FLT for exponent 3.

We will actually prove that

$$\alpha^3 + \beta^3 + \gamma^3 = 0$$

has no solutions in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-3})$, for $\alpha\beta\gamma \neq 0$. This is a more general result as $\mathbb{Z} \subseteq \mathcal{O}_K$ and we can always write

$$x^3 + y^3 + (-z)^3 = 0$$

if x, y, z were a solution to the equation

$$x^3 + y^3 = z^3.$$

To simplify notation, set $u = \frac{-1 \pm \sqrt{-3}}{2}$, which we saw before is in $\mathcal{O}_K$ and is in fact a unit. It satisfies the equation

$$u^2 + u + 1 = 0.$$

and so

$$u^3 = 1.$$

Thus, the units of $\mathcal{O}_K$ are given by

$$\pm 1, \ \pm u, \ \pm u^2$$

(check as an exercise!)

Observe that $N(\sqrt{-3}) = 3$ and so $\sqrt{-3}$ is a prime of K.

We set $\varpi = \sqrt{-3}$ as well to ease notation. The associate of ϖ are $\pm(1-u)$, $\pm(1-u^2)$, $\pm(u-u^2) = \pm\varpi = \pm\sqrt{-3}$

(again, check as an exercise!)

<u>Lemma 1</u>: Let $\alpha \in \mathcal{O}_K$. Then modulo ϖ α is congruent to 0 or ± 1.

<u>Proof</u>: We can write $\alpha = \frac{a+b\varpi}{2}$ with $a \equiv b \pmod 2$.

We know that $\frac{b+a\varpi}{2}$ is also in $\mathcal{O}_K$ by our characterization of $\mathcal{O}_K$. Thus,

$$\frac{1}{2}(a+b\varpi) = \cancel{\quad\quad}$$

$$= \frac{1}{2}(b+a\varpi)\varpi + 2a \qquad \text{(check this!)}$$

$$\equiv 2a \pmod{\varpi}.$$

We know that $2a \in \mathbb{Z}$ and everything in $\mathbb{Z}$ is congruent to $0, \pm 1$ mod 3. Since $\varpi \mid 3$ ~~and is prime~~, we have $\frac{1}{2}(a+b\varpi) \equiv 0, \pm 1 \pmod{\varpi}$. ∎

<u>Lemma 2</u>: Let $\alpha, \beta \in \mathcal{O}_K$ w/ $\varpi \nmid \alpha$, $\varpi \nmid \beta$.

① If $\alpha \equiv 1 \pmod{\varpi}$, then $\alpha^3 \equiv 1 \pmod{\varpi^4}$.

② If $\alpha \equiv -1 \pmod{\varpi}$, then $\alpha^3 \equiv -1 \pmod{\varpi^4}$

③ If $\alpha^3 + \beta^3 \equiv 0 \pmod{\varpi}$, then $\alpha^3 + \beta^3 \equiv 0 \pmod{\varpi^4}$

④ If $\alpha^3 - \beta^3 \equiv 0 \pmod{\varpi}$, then $\alpha^3 - \beta^3 \equiv 0 \pmod{\varpi^4}$.

Proof: Observe that $\varpi^4 = 9$ as we will use this fact.

① & ②: We have that $\alpha \equiv \pm 1 \pmod{\varpi}$ by Lemma 1.

So $\exists\, \beta \in \mathcal{O}_K$ s.t. $\alpha = \pm 1 + \beta\varpi$. Suppose $\alpha \equiv 1 \pmod{\varpi}$.

Then $\alpha = 1 + \beta\varpi$, and so

$$\alpha^3 = (1+\beta\varpi)^3 = 1 + 3\beta\varpi - 9\beta^2 + \beta^3\varpi^3$$
$$\equiv 1 + 3\beta\varpi + \beta^3\varpi^3 \pmod{\varpi^4}.$$

We also have (since $-3 = \varpi^2$)

$$3\beta\varpi + \beta^3\varpi^3 = \varpi^3(\beta^3 - \beta)$$
$$= \varpi^3\beta(\beta-1)(\beta+1).$$

Lemma 1 gives that $\beta(\beta-1)(\beta+1) \equiv 0 \pmod{\varpi}$ and so

$\varpi^3\beta(\beta-1)(\beta+1) \equiv 0 \pmod{\varpi^4}$. Thus,

$$\alpha^3 \equiv 1 \pmod{\varpi^4}.$$

The same arg gives ② as well.

③+④: $\alpha^3 - \alpha = \alpha(\alpha-1)(\alpha+1) \equiv 0 \pmod{\varpi}$ by lemma 2.

$\Rightarrow \alpha^3 + \beta^3 \equiv \alpha + \beta \pmod{\varpi}$

If $\alpha \equiv 1 \pmod{\varpi}$, then $\beta \equiv -1 \pmod{\varpi}$ and vice versa.

$\Rightarrow$ by ① & ② that we have $\alpha^3 \equiv 1 \pmod{\varpi^4}$ and $\beta^3 \equiv -1 \pmod{\varpi^4}$.

$\Rightarrow \alpha^3 + \beta^3 \equiv 0 \pmod{\varpi^4}$

This same type of arg gives ④ as well. ∎

Lemma 3: Let $\alpha, \beta, \gamma \in \mathcal{O}_K$ and suppose $\alpha^3 + \beta^3 + \gamma^3 = 0$. If $\gcd(\alpha, \beta, \gamma) = 1$ then ϖ divide one and only one of α, β, γ.

Proof: Suppose ϖ divides none of them. Then the previous Lemma 1 & 2 ① & ⑤ give

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\varpi^4}$$

Thus, ϖ^4 divides $3, 1, -1$ or -3. However $\varpi^4 = 9$ so this is a contradiction. Thus ϖ divides $\alpha, \beta,$ or γ. It is clear it cannot divide 2 of them for if it did then

$$\alpha^3 + \beta^3 + \gamma^3$$

would imply it divided all three $\Rightarrow \varpi \mid \gcd(\alpha, \beta, \gamma) = 1$. ☒

Lemma 4: Suppose $\exists$ nonzero $\alpha, \beta, \gamma \in \mathcal{O}_K$ with $\varpi \nmid \alpha\beta\gamma$, and units $\varepsilon_1, \varepsilon_2$ and a pos integer r s.t.

$$\alpha^3 + \varepsilon_1 \beta^3 + \varepsilon_2 (\varpi^r \gamma)^3 = 0.$$

Then $\varepsilon_1 = \pm 1$ and $r \geq 2$.

Proof: Since r is a positive integer, we have

$$\alpha^3 + \varepsilon_1 \beta^3 \equiv 0 \pmod{\varpi^3}.$$

Lemma 2 gives

$$\alpha^3 + \varepsilon_1 \beta^3 \equiv \pm 1 + \varepsilon_1 (\pm 1) \equiv 0 \pmod{\varpi^3}.$$

We know the unit ε_1 must be $\pm 1, \pm u, \pm u^2$, and so plugging in all possibilities we get

ϖ^3 divides, $\pm 2, 0, \pm(1 \pm u), \pm(1+u^2)$ with all possible combinations of signs. We claim this cannot happen ~~unless~~ except in the case $\pm 1 \pm \varepsilon_1(\pm 1) \equiv 0 \pmod{\varpi^3}$.

$\pm 1 \pm \varepsilon_1(\pm 1) = \pm 2$: In this case $N(\pm 1 \pm \varepsilon_1(\pm 1)) = 4$ and

$N(\varpi^3) = 27$, so $\varpi^3 \nmid \pm 2$.

$\pm 1 + \varepsilon_1(\pm 1) = 1-u, 1-u^2$: Since $1-u$ and $1-u^2$ are associates of ϖ, this would give $\varpi^3 | \varpi$, #

$\pm 1 + \varepsilon_1(\pm 1) = 1+u, 1+u^2$: $1+u = -u^2$, $1+u^2 = -u$, these are both units but ϖ^3 is not a unit, so cannot divide a unit.

Thus we must have $\alpha^3 + \varepsilon_1 \beta^3 \equiv 0 \pmod{\varpi^3} \Rightarrow$ by Lemma 2 ③ that $\alpha^3 + \varepsilon_1 \beta^3 \equiv 0 \pmod{\varpi^4}$. Thus, $\varpi^4 \mid \varepsilon_2(\varpi^r \gamma)^3$

$\Rightarrow r \geq 2$. ∎

__Lemma 5:__ There do not exist nonzero $\alpha, \beta, \gamma \in \mathcal{O}_K$, a unit ε, and an integer $r \geq 2$ such that

$$\alpha^3 + \beta^3 + \varepsilon(\varpi^r \gamma)^3 = 0. \qquad (*)$$

This ~~lk~~ lemma is essentially where our work remains. Before we prove it we see how it gives us the Theorem we desire:

Thm: There are no nonzero $\alpha, \beta, \gamma \in \mathcal{O}_K$ s.t

$$\alpha^3 + \beta^3 + \gamma^3 = 0.$$

Proof: Suppose $\exists\ \alpha, \beta, \gamma \in \mathcal{O}_K$ nonzero w/

$$\alpha^3 + \beta^3 + \gamma^3 = 0.$$

Divide out by $\gcd(\gamma, \beta, \alpha)$ so that we can now assume $\gcd(\alpha, \beta, \gamma) = 1$. Lemma 3 gives that ϖ divides exactly one of α, β, γ, say $\varpi \mid \gamma$. Let $\varpi^r \| \gamma$ (this means r is the largest integer so that $\varpi^r \mid \gamma$). Then $\gamma = \varpi^r \gamma_1$ w/ $\gcd(\varpi, \gamma_1) = 1$, $\gamma_1 \in \mathcal{O}_K$. Lemma 4 gives $r \geq 2$ and we have

$$\alpha^3 + \beta^3 + (\varpi^r \gamma_1)^3 = 0.$$

This contradicts lemma 5. ∎

Thus it only remains to prove lemma 5:

Proof (lemma 5): We prove this by descent. Since our solutions cannot be ordered themselves, our descent proceeds via the norm of the elements. Suppose $\alpha, \beta, \varpi^r \gamma$ is a solution. We may assume wlog $\gcd(\alpha, \beta, \varpi^r \gamma) = 1$. And $\gcd(\varpi, \gamma) = 1$.

We have

$$\alpha^3+\beta^3 \equiv 0 \pmod{\varpi^{3r}}$$

with $3r \geq 6$.

We can factor $\alpha^3+\beta^3$ in $\mathcal{O}_K$ as

$$\alpha^3+\beta^3 = (\alpha+\beta)(\alpha+u\beta)(\alpha+u^2\beta).$$

Claim: If $\wp$ is a prime so that $\wp$ divides two of $\alpha+\beta$, $\alpha+u\beta$, $\alpha+u^2\beta$ then $\wp$ is an associate of ϖ.

Pf: There are several case to check, all pretty much the same. For example, if $\wp \mid \alpha+\beta$ and $\wp \mid \alpha+u\beta$, then $\wp \mid (\alpha+\beta)-(\alpha+u\beta) = \beta(1-u)$. Similarly, $\wp \mid \alpha(1-u)$. However, $\gcd(\alpha,\beta)=1 \Rightarrow \wp \mid 1-u$ which is an associate of ϖ. Thus, $\wp$ is an associate of ϖ. The other cases are analogous. □

Using this same type of arg. one can use $\varpi \nmid \beta$ to show that the difference between $\alpha+\beta$, $\alpha+u\beta$, $\alpha+u^2\beta$ is divisible by ϖ but not ϖ^2. This shows that 2 of the three can only be divisible by ϖ. For if 2 of the three were divisible by ϖ^2, their difference would be.

Thus we have if we let $a,b,c \in \mathbb{Z}$ s.t.

$\varpi^a \| \alpha+\beta$, $\varpi^b \| \alpha+u\beta$, $\varpi^c \| \alpha+u^2\beta$, then we have $\{a,b,c\} = \{1,1,3r-2\}$ since $a+b+c=3r$. Thus,

$$\frac{\alpha+\beta}{\varpi^a}, \quad \frac{\alpha+u\beta}{\varpi^b}, \quad \frac{\alpha+u^2\beta}{\varpi^c}$$

are elements of $\mathcal{O}_k$ with no common prime factors.

Thus, we have that equation (*) can be written as

$$\left(\frac{\alpha+\beta}{\varpi^a}\right)\left(\frac{\alpha+u\beta}{\varpi^b}\right)\left(\frac{\alpha+u^2\beta}{\varpi^c}\right) = -\varepsilon\gamma^3 \qquad (2).$$

This gives that each element on the LHS of equation (2) must be an associate of a cube in $\mathcal{O}_k$:

$$\begin{aligned} \alpha+\beta &= \varepsilon_1 \varpi^a \lambda_1^3 \\ \alpha+u\beta &= \varepsilon_2 \varpi^b \lambda_2^3 \qquad (3) \\ \alpha+u^2\beta &= \varepsilon_3 \varpi^c \lambda_3^3 \end{aligned}$$

with ε_i units.

Using that $u^3=1$ we have:

$$(\alpha+\beta) + u(\alpha+u\beta) + u^2(\alpha+u^2\beta)$$
$$= (\alpha+\beta)(1+u+u^2) = 0.$$

Thus, we have

$$\varepsilon_1 \varpi^a \lambda_1^3 + \varepsilon_4 \varpi^b \lambda_2^3 + \varepsilon_5 \varpi^c \lambda_3^3 = 0 \qquad (3)$$

where $\varepsilon_4 = u\varepsilon_2$, $\varepsilon_5 = u^2\varepsilon_3$ are units.

Equation (3) is symmetric in a, b, c so we can set $a=1$, $b=1$, $c=3r-2$.

which gives:

$$\varepsilon_1 \varpi \lambda_1^3 + \varepsilon_4 \varpi \lambda_2^3 + \varepsilon_5 \varpi^{3r-2} \lambda_3^3 = 0.$$

Dividing by $\varepsilon_1 \varpi$:

$$\lambda_1^3 + \varepsilon_6 \lambda_2^3 + \varepsilon_7 \left(\varpi^{\cancel{3r}\, r-1} \lambda_3 \right)^3 = 0 \qquad (4)$$

where $\varepsilon_6 = \varepsilon_4/\varepsilon_1$, $\varepsilon_7 = \varepsilon_5/\varepsilon_1$ are units.

Since $\gamma \neq 0$, equations (2) and (3) give $\lambda_1 \lambda_2 \lambda_3 \neq 0$.

Lemma 4 now gives $\varepsilon_6 = \pm 1$ and $r-1 \geq 2$. However, equation (4) is of the form (*) because $\varepsilon_6 \lambda_2^3$ is either λ_2^3 or $(-\lambda_2)^3$ ($\varepsilon_6 = \pm 1$). We have

$$N(\lambda_1^3 \lambda_2^3 \varpi^{3r-3} \lambda_3) = N\left(\varpi^{-3} (\alpha+\beta)(\alpha+u\beta)(\alpha+u^2\beta)\right)$$

$$= N(\varpi^{3r-3}\gamma^3) < N(\alpha^3 \beta^3 \varpi^{3r} \gamma^3)$$

since $N(\varpi^{3r-3}) = N(\varpi)^{3r-3} = 3^{3r-3}$

and $N(\alpha^3 \beta^3 \varpi^{3r}) = N(\alpha) N(\beta)\, 3^{3r}$ and $N(\alpha), N(\beta) \geq 1$

and $3^{-3} < 1$.

Thus, from our original solution $\alpha, \beta, \varpi^r \gamma$ we produce another nonzero solution in $\mathcal{O}_K$ w/ strictly smaller norm. However, the value of a norm for a nonzero element of $\mathcal{O}_K$ is a positive integer. Repeating this process produces a strictly decreasing sequence of positive integers #. Thus there could be no solution to begin with. ☒