Abstract

This thesis deals with some special types of Diophantine equations. Two classic cases of Fermat's equation are shown to have no nontrivial integer solutions, using two different approaches. The rest of the thesis deals with some instances of $y^2 = x^3 + k$, commonly known as Mordell's equation. In most cases, no integer solutions exist.

Contents

1 Introduction

A Diophantine equation is a polynomial equation with integer coefficients in two or more variables, where we seek integer solutions. If the equation is linear, it can easily be solved using Euclid's algorithm or continued fractions. The nonlinear case is more difficult, and requires more thought and mathematical theory in order to find all solutions (or to prove that there isn't any!).

A common method to show that a Diophantine equation lacks solutions in positive integers is called infinite descent. The idea is this: One assumes that the given equation has an integer solution, and then shows that one can obtain another solution, where the value of one of the variables is smaller. One can then redo the same argument on this new solution, to obtain another solution where the value of the variable is even smaller, and so on. This creates an infinite decreasing sequence of positive integers. But by the Well-ordering Axiom, every nonempty set of positive integers has a smallest element, and so every decreasing sequence of positive integers is finite (if nothing else, it has to end with 1). This means that we would sooner or later come to a point where we could no longer find a smaller solution, and hence that there cannot exist a solution to start with.

Chapter 2 concerns the lack of integer solutions to $x^4 + y^4 = z^4$, which was the first case of Fermat's Last Theorem to be proved (in fact by Fermat himself!). It also includes a study of the closely related equation $x^4 - y^4 = z^2$. Chapter 3 deals with equations of the form $y^2 = x^3 + k$, which is called Mordell's equation (sometimes Bachet's equation). The equation is studied using two different approaches, and in most cases it will be shown that no integer solutions exist. Our discussion is heavily based on [7], and in most cases we have merely filled in the details in Mordell's sparsely formulated proofs. Chapter 4 contains a proof that Fermat's equation lacks integer solutions for $n = 3$, using the theory developed in Chapter 3.2. At last we have an Appendix where some of the k values from Chapter 3.1 are explicitly computed.

The reader is assumed to have basic knowledge of elementary number theory and ring theory.

2 Quartic equations

2.1 Fermat's equation for $n = 4$

In this section, we show that the equation $x^4 + y^4 = z^4$ has no nontrivial integer solutions, using infinite descent, which seems to have been Fermat's favorite method. He went as far as to claim that all his assertions could be proved (and that he had proofs of them) using infinite descent. However, the only one of his proofs that is actually known is that of $x^4 + y^4 = z^4$ lacking integer solutions (he proves the statement that the area of a right triangle with rational sides cannot be a rational square, but this is equivalent, see chapter 22 of [3]). After Fermat, many other mathematicians proved similar results, including Euler.

We begin our discussion with a simple, yet useful Lemma.

Lemma 2.1. *Let $a, b, c \in \mathbb{Z}$ and $ab = c^n$. If $gcd(a, b) = 1$, then a and b are n:th powers as well.*

Proof. By unique factorization, we have that $a = p_1^{k_1} \cdots p_r^{k_r}, b = q_1^{l_1} \cdots, q_s^{l_s}$ and $c^n = r_1^{nm_1} \cdots r_t^{nm_t}$, for some primes p_i, q_i, r_i. Since a and b are relatively prime, each factor r_i in c^n that divides a must do so to its full power, a multiple of n. The same holds for b. Hence the powers of the factors of c^n are completely split between a and b, which means that a and b must be n:th powers as well. □

Theorem 2.2. *$x^4 + y^4 = z^2$ has no nontrivial integer solutions.*

Proof. We may assume that $\gcd(x, y) = 1$, for if $\gcd(x, y) = d$ it follows that $d^2|z$, and then we can reduce the equation to $x_1^4 + y_1^4 = z_1^2$ with $\gcd(x_1, y_1) = 1$. The next observation is that $x \not\equiv y \mod 2$. If both are odd, we get $x^4 + y^4 \equiv 2 \mod 4$, which is a contradiction since squares are $\equiv 0, 1 \mod 4$. If both are even, then $\gcd(x, y) > 1$, and our previous argument can be applied.

Assume that $x^4 + y^4 = z^2$ has a solution (x, y, z), where y is even and x, z are odd, and rewrite the equation as $y^4 = (z - x^2)(z + x^2)$. Any prime that divides both factors must also divide their sum and difference, $2z$ and $2x^2$. Since $\gcd(x, z) = 1$, it follows that $\gcd(z-x^2, z+x^2) = 2$, so that $\gcd\left(\frac{z-x^2}{2}, \frac{z+x^2}{2}\right) = 1$. Then by Lemma (2.1), we get two cases:

$$\begin{cases} z - x^2 = 2a^4 \\ z + x^2 = 8b^4 \\ a \equiv 1 \mod 2 \\ \gcd(a, b) = 1 \end{cases} \quad \text{or} \quad \begin{cases} z - x^2 = 8b^4 \\ z + x^2 = 2a^4 \\ a \equiv 1 \mod 2 \\ \gcd(a, b) = 1 \end{cases}$$

The first case implies that $x^2 = -a^4 + 4b^4 \implies 1 \equiv -1 \mod 4$, which is impossible. So the second case holds, and it implies $4b^4 = (a^2 - x)(a^2 + x)$. Arguing as before, we get that $\gcd\left(\frac{a^2-x}{2}, \frac{a^2+x}{2}\right) = 1$. Hence $\frac{a^2-x}{2} = c^4$, $\frac{a^2+x}{2} = d^4$, which implies $c^4 + d^4 = a^2$. We have that $c \not\equiv d \mod 2$, since a is odd, and obviously $\gcd(c, d) = 1$.

Thus, the triple (c, d, a) solves the original equation, and has a strictly smaller right hand side. Here comes the descent: we can apply the same reasoning to our new solution again and again. This will create an infinite, decreasing sequence of positive integers (right-hand sides), which is impossible by the well-ordering axiom. Hence there cannot exist any nontrivial integer solutions to start with. □

Corollary 2.3. *$x^4 + y^4 = z^4$ has no nontrivial integer solutions.*

Proof. If such a solution (x_0, y_0, z_0) exists, then it corresponds to a solution (x_0, y_0, z_0^2) of the previous equation, which cannot exist by Theorem (2.2). □

2.2 The equation $x^4 - y^4 = z^2$

Following [1], we will study this equation with the aid of Pythagorean triples. As we will see, it is a rather natural approach.

Definition 2.1. *A Pythagorean triple is a triple $(x, y, z) \in \mathbb{N}^3$ that solves the equation $x^2 + y^2 = z^2$. If $gcd(x, y, z) = 1$, the triple is called primitive.*

Theorem 2.4. *$(x, y, z) \in \mathbb{N}^3$ is a primitive Pythagorean triple, with x even, if and only if there exists $s, t \in \mathbb{N}$ such that*

$$x = 2st, y = s^2 - t^2, z = s^2 + t^2$$
$$s > t > 0, s \not\equiv t \mod 2, gcd(s, t) = 1$$

Proof. The condition $\gcd(x, y, z) = 1$ implies that $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$. Together with the fact that x is even, this implies that y and z must be odd. Hence $z - y$ and $z + y$ are both even, say $z - y = 2u, z + y = 2v$, so that

$$x^2 = z^2 - y^2 = (z - y)(z + y) \iff \left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv$$

Note that $\gcd(u, v) = 1$ since it must divide the relatively prime numbers $u+v = z$ and $u - v = y$. Hence, by Lemma (2.1) we have

$$z = v + u = s^2 + t^2$$
$$y = v - u = s^2 - t^2$$
$$x^2 = 4vu = (2st)^2 \implies x = 2st$$

Finally, note that $\gcd(s,t)$ must divide $\gcd(y,z) = 1$, so that s, t are relatively prime. Also, $s \not\equiv t \mod 2$, because otherwise we would have $y \equiv z \equiv 0 \mod 2$, contrary to our assumption.

For the other direction, assume that x, y, z are given in terms of s and t. It is then easy to verify that

$$x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2 = z^2$$

so that they indeed form a Pythagorean triple. If $d = \gcd(x,y,z) > 1$, then any prime divisor of d must also divide $z + y = 2s^2$ and $z - y = 2t^2$. But this is impossible since $d \neq 2$ (x is the only even one), and $\gcd(s,t) = 1$. Hence $\gcd(x,y,z) = 1$, so the triple is primitive. □

Now we can use this together with the method of infinite descent to prove our main theorem, whose proof unfortunately require many different letters.

Theorem 2.5. *The equation $x^4 - y^4 = z^2$ has no nontrivial integer solutions.*

Proof. If $\gcd(x,y) = d$, we can write $x = dx_1, y = dy_1$ where $\gcd(x_1, y_1) = 1$. It follows that $d^2 | z$, and we can reduce the equation to $x_1^4 - y_1^4 = z_1^2$. Hence we might as well let $\gcd(x,y) = 1$. Now assume that the equation has at least one solution in positive integers, and pick the solution x_0, y_0, z_0 with the smallest possible value of x_0. Since we assume $\gcd(x_0, y_0) = 1$, x_0, y_0 cannot both be even. Also, to ensure that x_0 is minimal, it has to be odd (otherwise $\frac{x_0}{2}$ would be a smaller value). Hence, two cases arise, depending on whether y_0 is odd or even.

In the first case, where y_0 is odd, z_0 will be even. We can then rewrite the equation as $z_0^2 + (y_0^2)^2 = (x_0^2)^2$ and apply Theorem (2.4) to get

$$\begin{aligned} z_0 &= 2st \\ y_0^2 &= s^2 - t^2 \\ x_0^2 &= s^2 + t^2 \end{aligned}$$

where $s > t > 0$ and $\gcd(s,t) = 1$. But then $s^4 - t^4 = (s^2+t^2)(s^2-t^2) = (x_0 y_0)^2$, so that $(s, t, x_0 y_0)$ is a solution to the equation, where $0 < s = \sqrt{s^2 + t^2} = x_0$. This contradicts the minimality of x_0.

Next, if y_0 is even, z_0 will be odd, so a little rearranging allows us to use Theorem (2.4) again to obtain

$$\begin{aligned} y_0^2 &= 2st \\ x_0^2 &= s^2 + t^2 \\ z_0 &= s^2 - t^2 \end{aligned}$$

where again $s > t > 0$ and $\gcd(s,t) = 1$. We may assume that s is even while t is odd (assuming that s is odd and t is even gives the same result), so that

$\gcd(2s, t) = 1$. Then by Lemma (2.1), we get $2s = w^2, t = v^2$, and since w is even as well, $w = 2u$. This gives that $s = \frac{w^2}{2} = \frac{4u^2}{2} = 2u^2$, and consequently $x_0^2 = s^2 + t^2 = (2u^2)^2 + (v^2)^2$. We can then apply Theorem (2.4) yet again to obtain

$$\begin{aligned} 2u^2 &= 2ab \\ v^2 &= a^2 - b^2 \\ x_0 &= a^2 + b^2 \end{aligned}$$

where $a > b > 0$ and $\gcd(a, b) = 1$. Also, $a = c^2, b = d^2$ by Lemma (2.1). Hence we can write $c^4 - d^4 = a^2 - b^2 = v^2$, so that (c, d, v) is a solution of the equation, with $0 < c = \sqrt{a} < a^2 + b^2 = x_0$. But this is another contradiction to the minimality of x_0. Hence, if there exists a solution with smallest possible x_0, we can in any case find a smaller one. This contradicts the well-ordering axiom, and so no nontrivial integer solutions can exist. □

Corollary 2.6. *The equation $x^4 + y^4 = 2z^2$ has no nontrivial integer solutions.*

Proof. Squaring both sides, subtracting $4(xy)^4$ and dividing by 4, we obtain the equation $z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2$, which is of the form dealt with in Theorem (2.5). Its trivial solution $(x, y, z) = (\pm 1, \pm 1, \pm 1)$ corresponds to the trivial solution $\left(z, xy, \frac{x^4 - y^4}{2}\right) = (\pm 1, \pm 1, 0)$ of the previous equation. □

3 Mordell's equation, $y^2 = x^3 + k$

Just as the previous section, this section also begins with Fermat. He claimed that $(x, y) = (3, \pm 5)$ is the only solution to the equation when $k = -2$ and that $(x, y) = (2, \pm 2), (5, \pm 11)$ are the only solutions when $k = -4$. As usual however, he never published any proofs of this. In the following centuries, many mathematicians proved the nonexistence of solutions for certain values of k. See chapter 20 of [3] for many historical references. The study of the equation eventually led to many important developments in algebraic number theory, and in the 20th century, the equation was studied in greater generality. One of the most prominent mathematicians working on it was Louis Mordell, after whom the equation is commonly named.

We will study the existence or nonexistence of integer solutions using two different approaches. First using some congruence arguments, where the assumption of integer solutions leads to the absurdity that x lies in no congruence class modulo 4 or modulo 8. Then, we will use some arguments from abstract algebra, relying on the arithmetical properties of more general rings than $\mathbb{Z}$ called Euclidean domains. Both methods are due to [7].

3.1 Eliminating Congruence Classes

We begin this section with a lemma that will frequently be used in the following proofs. We introduce the notation $p^n||x$, which means that p^n is the largest power of p that divides x.

Lemma 3.1. *Let p be an odd prime s.t. $p|y^2 - kb^2$ and $(k/p) = -1$. Then:*
a) $p^\alpha||y$ and $p^\beta||b$ for some exponents $\alpha, \beta > 0$.
b) Let $\gamma = min\{\alpha, \beta\}$. Then $p^{2\gamma}||y^2 - kb^2$.

Proof. a) Assume that p does not divide both y and b. Then since $y^2 - kb^2 \equiv 0 \mod p$, which is equivalent to $y^2 \equiv kb^2 \mod p$, it divides neither. But this allows us to use the Legendre symbol to obtain

$$1 = (y^2/p) = (kb^2/p) = (k/p)$$

which contradicts our assumption.

b) By part a), we can write $y^2 = p^{2\alpha}y_1^2, b^2 = p^{2\beta}b_1^2$, where p divides none of y_1, b_1. When we divide $y^2 - kb^2$ by $p^{2\gamma}$, we get three cases, depending on the order relation between α and β. The first two cases where $\alpha \neq \beta$ lead to $p^{2(\alpha-\beta)}y_1^2 - kb_1^2$ and $y_1^2 - kp^{2(\beta-\alpha)}b_1^2$ respectively. None of these expressions can be $\equiv 0 \mod p$ since p divides none of y_1, k, b_1. In the case $\alpha = \beta$ we get $(\frac{y}{p^\gamma})^2 - k(\frac{b}{p^\gamma})^2 = y_1^2 - kb_1^2$. If we assume that $y_1^2 - kb_1^2 \equiv 0 \mod p$, then $y_1^2 \equiv kb_1^2 \mod p$, and since p divides none of y_1, k, b_1, we can use the proof of part a) to arrive at a contradiction. □

Theorem 3.2. *The equation $y^2 = x^3 + 45$ has no integer solutions.*

Proof. We prove this by eliminating congruence classes of $x \mod 8$. First, we note that x cannot be $\equiv 0 \mod 2$. If that were the case, it would follow that $y^2 \equiv 5 \mod 8$, which is impossible since squares are $\equiv 0, 1, 4 \mod 8$. This eliminates all even congruence classes. We also cannot have $x \equiv 1 \mod 4$, since it would imply $y^2 \equiv 2 \mod 4$, which is impossible since squares are $\equiv 0, 1 \mod 4$. Hence we are left with the cases $x \equiv 3, 7 \mod 8$.

Rewrite the equation as $y^2 - 72 = x^3 - 27 = (x-3)(x^2+3x+9)$, and call the second factor R. We claim that $x \not\equiv 0 \mod 3$, so that $x - 3 \not\equiv 0 \mod 3$, which will be of importance later on. If we assume the converse, then $y^2 - 72 \equiv y^2 \equiv 0 \mod 3$ so that $x \equiv y \equiv 0 \mod 3$. This implies that $x = 3x_1, y = 3y_1$ for some integers x_1, y_1. Our equation then becomes $9y_1^2 - 72 = 27x_1^3 - 27$ which simplifies to $y_1^2 = 3x_1^3 + 5$. But this equation has no solutions, which can be seen by reducing $\mod 3$.

Now assume that $x \equiv 3 \mod 8$, so that $R = x^2 + 3x + 9 \equiv 3 \mod 8$ as well. Then R contains at least one prime $p \equiv \pm 3 \mod 8$ (if not, every prime factor of R would be $\equiv \pm 1 \mod 8$, so that $R \equiv \pm 1 \mod 8$ as well, contrary to assumption). At least one such prime must occur to an odd power, because otherwise we would have $R \equiv (\pm 1)^m (\pm 3)^{2n} \equiv \pm 1 \mod 8$, which again contradicts our assumption.

Under these assumptions we must have $p | y^2 - 72$. Since we also have $(2/p) = -1$ for such a prime, Lemma (3.1) gives that $p^{2\alpha} | y^2, p^{2\beta} | 72$ and $p^{2\gamma} || y^2 - 72$, where $\gamma = min\{\alpha, \beta\}$. Since $72 = 2^3 \times 3^2$, we must have that $p = 3$ and $\gamma = 1$. But this means that $x^2 + 3x + 9 \equiv 0 \mod 3$, which is impossible since $x \not\equiv 0 \mod 3$.

In the case where $x \equiv 7 \mod 8$, we rewrite the equation as $y^2 - 18 = x^3 + 27 = (x+3)(x^2 - 3x + 9)$. Then $x^2 - 3x + 9 \equiv -3 \mod 8$, and hence contains at least one prime $q \equiv \pm 3 \mod 8$ to an odd power, so that $q | y^2 - 18$ as well. Since $(2/q) = -1$, Lemma (3.1) gives that $q | y$, and since $18 = 2 \times 3^2$, we see that $q = 3$. But this implies that $3 | x$ as well, and we have a contradiction. Hence there can be no integer solutions. □

Next, we move on to some equations where k is given by two integer parameters a, b.

Theorem 3.3. *The equation $y^2 + 4a^2 = x^3 + (4b-1)^3$ has no integer solutions, if a has no prime factors $p \equiv 3 \mod 4$.*

Proof. If $x \equiv 0 \mod 2$, then $y^2 \equiv 3 \mod 4$, and if $x \equiv 3 \mod 4$ then $y^2 \equiv 2 \mod 4$. Both cases are impossible since squares are $\equiv 0, 1 \mod 4$. Hence a solution can exist only if $x \equiv 1 \mod 4$

Write $x^3 + (4b-1)^3 = (x + (4b-1))(x^2 - (4b-1)x + (4b-1)^2)$. Then $(x^2 - (4b-1)x + (4b-1)^2) \equiv 3 \mod 4$, and hence contains an odd number of prime factors $p \equiv 3 \mod 4$. Then also $y^2 + 4a^2 \equiv 0 \mod p$ or equivalently, $y^2 \equiv -(2a)^2 \mod p$. Since we also have $(-1/p) = -1$ for such primes p, Lemma (3.1) gives that $p|a$. But this is a contradiction, and hence there can be no integer solutions. □

Theorem 3.4. *The equation $y^2 + (2a+1)^2 = x^3 + (4b+2)^3$ has no integer solutions, if $(2a+1)$ has no prime factors $p \equiv 3 \mod 4$.*

Proof. Almost identical to the proof of the previous Theorem. □

Theorem 3.5. *The equation $y^2 - 2b^2 = x^3 - a^3$ has no integer solutions, where $a \equiv 2, 4 \mod 8, b \equiv 1 \mod 2$, and b has no prime factor $p \equiv \pm 3 \mod 8$.*

Proof. Factor the right hand side as $(x-a)(x^2+ax+a^2)$. Note that x cannot belong to any even congruence class modulo 8, since it would imply $y^2 \equiv 2b^2 \equiv 2 \mod 8$, which is impossible since squares are $\equiv 0, 1, 4 \mod 8$. Also, $x \not\equiv 1 \mod 4$, since it implies $y^2 \equiv 3 \mod 4$, which is also impossible. This leaves us with two remaining cases: $x \equiv -1, 3 \mod 8$

Assume that $x \equiv -1 \mod 8$, so that $x - a \equiv \pm 3 \mod 8$. Then it contains at least one prime $p \equiv \pm 3 \mod 8$ to an odd power (otherwise, the powers of all prime divisors would be $\equiv \pm 1$, so that $x - a \equiv \pm 1$, contrary to assumption). Hence $p|y^2 - 2b^2$ as well. But since we also have $(2/p) = -1$, we can use Lemma (3.1) to get $p|b$, which is a contradiction. Next, assume that $x \equiv 3 \mod 8$, so that $x^2+ax+a^2 \equiv \pm 3 \mod 8$. Then it must contain some prime $q \equiv \pm 3 \mod 8$ to an odd power, and we can argue as before to once again get a contradiction to Lemma (3.1).

□

A similar result is:

Theorem 3.6. *The equation $y^2 + 2b^2 = x^3 - a^3$ has no integer solutions, if $a \equiv 4 \mod 8, b \equiv 1 \mod 2$, and b has no prime factor $p \equiv 5, 7 \mod 8$.*

Proof. If $x \equiv 0 \mod 2$, then $y^2 \equiv 2 \mod 4$ which is impossible. Hence $x \equiv 1, 3 \mod 4$. But if $x \equiv 1 \mod 4$, then $y^2 \equiv 3 \mod 4$ which is also impossible. Hence $x \equiv 3, 7 \mod 8$. But lastly, if $x \equiv 7 \mod 8$ then $y^2 \equiv 5 \mod 8$, another impossibility. This shows that a solution can exist only if $x \equiv 3 \mod 8$.

Factor the right hand side as $x^3 - a^3 = (x-a)(x^2+ax+a^2)$. Since $x - a \equiv -1 \mod 8$, it either contains some prime $p_i \equiv -1 \mod 8$ to an odd power, or some primes $q_i \equiv 3 \mod 8$ and $r_i \equiv -3 \mod 8$, each occurring to odd powers. We also have that $x^2 + ax + a^2 \equiv -3 \mod 8$, which means that it either contains some $r_i \equiv -3$ to an odd power, or some $p_i \equiv -1 \mod 8$ to an odd power.

Hence, in any case, some prime that is $\equiv 5, 7 \mod 8$ will divide $y^2 + 2b^2$. Since

$$(-2/p) = (-1/p)(2/p) = \begin{cases} 1, & \text{if } p \equiv 1, 3 \mod 8 \\ -1, & \text{if } p \equiv 5, 7 \mod 8 \end{cases}$$

we see that $(-2/p) = -1$, so that $p|b$ by Lemma (3.1). But this contradicts our assumption. Hence there are no integer solutions. □

Before we prove the next result, we need to define a generalization of the Legendre symbol known as the Jacobi symbol.

Definition 3.1. *Let $a,b \in \mathbb{Z}, b > 1, gcd(a, b) = 1$ and $b = p_1 \cdots p_r$ (odd primes, but not necessarily distinct). The Jacobi symbol (a/b) is then defined by $(a/b) = (a/p_1) \cdots (a/p_r)$, where the factors on the right hand side are Legendre symbols.*

Theorem 3.7. *Let b_1, b_2 be positive odd integers s.t. $gcd(a_1a_2, b_1b_2) = 1$. Then the Jacobi symbol (a/b) has the following properties:*
a) $a_1 \equiv a_2 \mod b \implies (a_1/b) = (a_2/b)$
b) $(a_1a_2/b) = (a_1/b)(a_2/b)$
c) $(a/b_1b_2) = (a/b_1)(a/b_2)$
d) $(a^2/b) = (a/b^2) = 1$
e) $(1/b) = 1$
f) $(-1/b) = (-1)^{\frac{b-1}{2}}$
g) $(2/b) = (-1)^{\frac{b^2-1}{8}}$
h) $(a/b)(b/a) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ *(generalized quadratic reciprocity law)*

Proof. a) If $a_1 \equiv a_2 \mod b$ and $b = p_1 \cdots p_r$, we can write $a_1 = kb + a_2 = k(p_1 \cdots p_r) + a_2 = k_1p_1 + a_2 = \cdots = k_rp_r + a_2$. That is, $a_1 \equiv a_2 \mod p_i$, $1 \leqslant i \leqslant r$. Hence $(a_1/b) = \prod_{i=1}^{r}(a_1/p_i) = \prod_{i=1}^{r}(a_2/p_i) = (a_2/b)$.

b) Since $\gcd(a_1a_2, p_i) = 1$ for each p_i dividing b, we have

$$(a_1a_2/b) = \prod_i (a_1a_2/p_i) = \prod_i (a_1/p_i) \prod_i (a_2/p_i) = (a_1/b)(a_2/b)$$

c) Let $b_1b_2 = p_1 \cdots p_n p_{n+1} \cdots p_r$ (not necessarily unique primes), where $p_1, \cdots p_n$ divide b_1 and $p_{n+1} \cdots p_r$ divide b_2. Then

$$(a/b_1b_2) = \prod_{i=1}^{r}(a/p_i) = \prod_{i=1}^{n}(a/p_i) \prod_{i=n+1}^{r} (a/p_i) = (a/b_1)(a/b_2)$$

d)

$$(a^2/b) = \prod_i (a^2/p_i) = \prod_i (a/p_i)^2 = \prod_i (a/p_i^2) = (a/b^2),$$

both symbols being equal to 1 since they are products of 1's.

e) $(1/b) = \prod_i (1/p_i) = 1$, since the congruence $x^2 \equiv 1 \mod p_i$ always has the solutions $x = 1, p_i - 1$.

f) We need the identity $\frac{x-1}{2} + \frac{y-1}{2} \equiv \frac{xy-1}{2} \mod 2$, where x and y are odd integers. Since x and y are odd, $(x-1)(y-1) = xy - x - y + 1 \equiv 0 \mod 4$. Hence $xy - 1 \equiv (x-1) + (y-1) \mod 4$, from which the identity follows upon division by 2. By using a property of the Legendre symbol, and repeatedly using the identity just shown, we get

$$(-1/b) = \prod_i (-1/p_i) = \prod_i (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_i \frac{p_i-1}{2}} = (-1)^{\frac{b-1}{2}}$$

as desired.

g) This is similar to the last one. We first show that $\frac{x^2-1}{8} + \frac{y^2-1}{8} \equiv \frac{(xy)^2-1}{8} \mod 2$, where x and y are odd integers. Clearly, $x^2 - 1$ and $y^2 - 1$ are both $\equiv 0 \mod 4$, so that $(x^2-1)(y^2-1) = (xy)^2 - x^2 - y^2 + 1 \equiv 0 \mod 16$, and hence $(xy)^2 - 1 \equiv (x^2-1) + (y^2-1)$, from which the result follows upon division by 8. By repeatedly using this identity, and another property of the Legendre symbol, we get

$$(2/b) = \prod_i (2/p_i) = \prod_i (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_i \frac{p_i-1}{8}} = (-1)^{\frac{b^2-1}{8}}$$

as desired.

h) Let $a = p_1 \cdots p_r, b = q_1 \cdots q_s$. Then, using previous parts of the theorem and the quadratic reciprocity law, we get:

$$\begin{aligned}(a/b)(b/a) &= \prod_{i=1}^{r}\prod_{j=1}^{s}(p_i/q_j)(q_j/p_i) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\ &= (-1)^{(\sum_{i=1}^{r}\frac{p_i-1}{2})(\sum_{j=1}^{s}\frac{q_j-1}{2})} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}\end{aligned}$$

□

We are now ready for the next, rather complicated example. In his statement of the theorem, Mordell unfortunately abuses notation slightly, since he introduces an integer parameter k. We avoid this by calling the same parameter c and let k have its usual meaning as the constant in $y^2 = x^3 + k$.

Theorem 3.8. *The equation $y^2 - cb^2 = x^3 - c^3a^3$ has no integer solutions under the following assumptions: $a \equiv -1 \mod 4, b \equiv 0 \mod 2$, c square-free, $c \equiv 3 \mod 4$, $gcd(c, b) = 1$, and if p is a prime such that $(c/p) = -1$, then p is not a common factor of a and b.*

Proof. First of all, to avoid the contradiction that $y^2 \equiv 2, 3 \mod 4$, we must have that $x \equiv 1 \mod 4$. Now write $y^2 - cb^2 = (x - ca)(x^2 + cax + c^2a^2)$, and let $F = x^2 + cax + c^2a^2$.

We claim that $\gcd(x, c) = 1$. Assume that there is a prime q that divides $\gcd(x, c)$. Then q divides x^3, c^3a^3 and cb^2, which implies that $q|y^2$ and, since q is prime, $q^2|y^2$. Furthermore, $q^2|F$, since it divides all the included terms. All this implies that $q^2|cb^2$. Since $q \nmid b$ ($q|c$, but $\gcd(c, b) = 1$), we must have that $q^2|c$, but this contradicts the fact that c is square-free. Hence $gcd(x, c) = 1$, which implies that $\gcd(F, c) = 1$. Now, using the previous theorem and that both F and c are $\equiv 3 \mod 4$, we get

$$(c/F)(F/c) = (-1)^{\frac{c-1}{2}\frac{F-1}{2}} = -1$$

so that

$$(c/F) = (c/F)(F^2/c) = -(F/c) = -(x^2/c) = -1$$

and consequently

$$-1 = (c/F) = \prod_i (c/p_i)$$

Hence F contains at least one prime $p \equiv 3 \mod 4$ to an odd power s.t. $(c/p) = -1$. This implies that $y^2 - cb^2 \equiv 0 \mod p$ as well. By yet another application of Lemma (3.1), we see that p occurs to an even power in $y^2 - cb^2$, so that p must occur to an odd power in $x - ca$. Hence $x - ca \equiv 0 \mod p$ so that $x \equiv ca \mod p$. By using this fact and that $F = x^2 + cax + c^2a^2 \equiv 0 \mod p$, we can do some rewriting to obtain $3cax \equiv 0 \mod p$. The last step of the proof is to show that p divides none of $3, c, a, x$.

If $p = 3$, then $b \equiv 0 \mod 3$. We also get that $-1 = (c/p) = (c/3)$ which can only happen if $c \equiv 2 \mod 3$, which implies that $b \not\equiv 0 \mod 3$ by assumption. This is clearly a contradiction. p cannot divide c, since $p|b$ but $\gcd(c, b) = 1$. p cannot divide a, since it divides b while a and b have no such prime in common. If $p|x$, or in other words, $x \equiv 0 \mod p$, we would get that $ca \equiv 0 \mod p$, which is impossible by what we just showed.

Hence we come to the contradiction that $3cax \equiv 0 \mod p$ even though p divides none of the factors. Therefore, the equation $y^2 - cb^2 = x^3 - c^3a^3$ has no integer solutions under the assumptions listed in the theorem. □

3.2 Arithmetic in Euclidean Domains

We begin this section by recalling some basic definitions from abstract algebra. An integral domain is a commutative ring that contains some 1_R (identity element under multiplication), but no zero divisors. A unit u in a ring R is an element for which there exists some $v \in R$ s.t. $uv = 1_R$. The product of any two units may not be 1_R, but such a pairing always exist. Hence the units in a ring form a group under multiplication. An element is called irreducible if it is not a unit, and only has itself and units as divisors (hence it is a generalization of the primes in $\mathbb{Z}$). Two elements $a, b \in R$ are called associates if $a = bu$ for some unit u.

Note that being associates is an equivalence relation. Clearly $a = a1_R$, so we have reflexivity. If $a = bu$ with u a unit, then $b = buv = av$ for some other unit v. Hence we have symmetry. Lastly, if $a = bu$ and $b = cv$, we get $a = bu = cuv = cw$ for some other unit w, so that we have transitivity as well.

Definition 3.2. *A Euclidean domain E is an integral domain equipped with a function $\delta : E \backslash 0_E \to \mathbb{Z}_+$ with the following properties:*
1) $\delta(a) \leqslant \delta(ab)$ for $a, b \in E$. Equality holds only if b is a unit.
2) for $a, b \in E, b \neq 0$, there exists $q, r \in E$ s.t. $a = bq + r$ and either $r = 0_E$ or $\delta(r) < \delta(b)$.

The second property can be seen as a generalization of the familiar division algorithm from the integers. In a Euclidean domain, we also have the following generalization of the fundamental theorem of arithmetic:

Theorem 3.9. *Every nonzero, nonunit element in a Euclidean domain is the product of irreducible elements. The product is unique up to associates.*

Proof. Let E be a Euclidean domain and let S be the set of nonzero nonunits in E that are not the products of irreducible elements. We will show that S must be empty. Assume it is not. Then the set $\{\delta(s) | s \in S\}$ is a nonempty set of nonnegative integers, which has a smallest element by the well-ordering axiom. In other words, $\exists a \in S$ s.t. $\delta(a) \leqslant \delta(s)$ for all $s \in S$. Since a is not irreducible, $a = bc$ for some nonunits $b, c \in E$. By definition of δ, $\delta(b) \leqslant \delta(bc)$, but we cannot have equality, since it would imply the contradiction that c is a unit. Hence $\delta(b) < \delta(bc) = \delta(a)$, which shows that $b \notin S$. By the same argument, $c \notin S$. But then b and c are products of irreducible elements, so a must be as well. Hence S is empty.

Now we show uniqueness. Assume that there exist two factorizations of some element $a \in E$, $p_1 \cdots p_r = q_1 \cdots q_s$, where each p_i and q_i is irreducible in E and $s \geqslant r$. p_1 must divide some q_i, say q_1 (perhaps after relabelling). Then $q_1 = p_1 k_1$. Since q_1 is irreducible, k_1 must be a unit. We can then cancel p_1 from both sides to get $p_2 \cdots p_r = k_1 q_2 \cdots q_s$. By the same argument, $p_2 | q_2$, so that $q_2 = k_2 p_2$, where again k_2 must be a unit. Carrying on like this, we will eventually arrive at $1 = k_1 \cdots k_r q_{r+1} \cdots q_s$. But this shows that the

remaining q_i's are units, so that $r = s$ and the factorization of a is unique up to associates. $\square$

Since being associates is an equivalence relation, we can create equivalence classes of associates, for example $[a] = \{b | b \text{ is associate of } a\}$. The uniqueness "up to associates" in the previous theorem then intuitively has to do with multiplication of equivalence classes. The product ab will still represent the same element if we replace a or b with any of their respective associates.

Theorem (3.9), together with a few other results (for details, see for example chapter 9 of [5]), gives the crucial property that any two elements in a Euclidean domain (not both zero) will have a greatest common divisor.

Definition 3.3. *The set $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is called the ring of Gaussian integers.*

The set of units in $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$, the complex 4:th roots of unity. Considering our purposes, the following result is not very surprising.

Theorem 3.10. *The ring of Gaussian integers is a Euclidean domain w.r.t $\delta(z) = |z|^2$.*

Proof. We show that $\delta(z)$ has the desired properties. For the first property, let $a = s + ti, b = u + vi$ be elements of $\mathbb{Z}[i]$. Then

$$\begin{aligned}\delta(ab) &= \delta((s+ti)(u+vi)) = \delta((su-tv)+(sv+tu)i) \\ &= (su-tv)^2 + (sv+tu)^2 = (s^2+t^2)(u^2+v^2) \\ &= \delta(a)\delta(b) \geqslant \delta(b)\end{aligned}$$

The last inequality is an equality only if a is a unit. This is equivalent to the statement that $\delta(a) = 1$ if and only if a is a unit, which is easy to prove. If a is a unit, it has an inverse a^{-1}. Hence $1 = \delta(1) = \delta(aa^{-1}) = \delta(a)\delta(a^{-1})$, so that $\delta(a) = 1$. The other direction is immediate, since $1 = \delta(a) = |a|^2$ implies that a is a unit.

For the proof of the second property, we temporarily move over to the larger ring $\mathbb{Q}[i]$ (which of course contains $\mathbb{Z}[i]$). For a, b as above, we have that

$$\frac{a}{b} = \frac{s+ti}{u+vi} = \frac{(s+ti)(u-vi)}{(u+vi)(u-vi)} = \frac{su+tv}{u^2+v^2} + \frac{tu-sv}{u^2+v^2}i$$

Let $c = \frac{su+tv}{u^2+v^2}, d = \frac{tu-sv}{u^2+v^2}$. Since $c, d \in \mathbb{Q}$, their distances to the nearest integer are at most $\frac{1}{2}$. More formally, $\exists m, n \in \mathbb{Z}$ s.t. $|m-c| \leqslant \frac{1}{2}$, $|n-d| \leqslant \frac{1}{2}$. Now,

$$\begin{aligned}a = b\frac{a}{b} &= b(c+di) = b((c+m-m)+(d+n-n)i) \\ &= b(m+ni) + b((c-m)+(d-n)i)\end{aligned}$$

which is of the form $bq + r$. We also have that

$$\begin{aligned}\delta(r) &= \delta(b)\delta((c-m)+(d-n)i) \\ &= \delta(b)((c-m)^2+(d-n)^2) \\ &\leqslant \delta(b)(\frac{1}{4}+\frac{1}{4}) < \delta(b)\end{aligned}$$

This completes the proof. □

Together with Theorem 3.9, we get the desired property that unique factorization holds in $\mathbb{Z}[i]$. In fact, the function $\delta(z) = |z|^2$ will work in all the domains that we will consider. Before applying this to Mordell's equation, we need two short lemmas.

Lemma 3.11. *Let E be a Euclidean domain with $\delta(z) = |z|^2$ and $a \in E$. If $\delta(a)$ is prime in $\mathbb{Z}$, then a is irreducible in E.*

Proof. We prove the contrapositive statement. Assume that $a \in E$ is not irreducible. Then $a = bc$ for some nonunits $b, c \in E$, and consequently $\delta(a) = |bc|^2 = |b|^2|c|^2 = \delta(b)\delta(c)$. If $\delta(a)$ were prime, then $\delta(b) = 1$ or $\delta(c) = 1$. But then b or c must be a unit, and we have a contradiction. □

Lemma 3.12. *Let E be a Euclidean domain, $a, b, c \in E$ and $ab = c^n$ for some unit u. If a and b are relatively prime, then they must be on the form $a = u_1\alpha^n, b = u_2\beta^n$ for some units u_1, u_2 and $\alpha, \beta \in E$.*

Proof. Being elements of a Euclidean domain, a, b and c are all products of irreducible elements, and possibly units. Since $\gcd(a, b) = 1$, a and b only have unit factors in common, and each irreducible factor of c^n occurs to its full power in either a or b. We have no control over possible unit factors of c, which may be split arbitrarily between a and b (that in turn may contain unit factors, of course). Since a product of units is a unit, we conclude that $a = u_1\alpha^n$ and $b = u_2\beta^n$ for some units u_1, u_2 and $\alpha, \beta \in E$. □

Theorem 3.13. *The only integer solution to $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.*

Proof. If x is even, then y is odd and consequently $y^2 \equiv 1 \mod 4$. This implies that $x^3 \equiv 2 \mod 4$, which is impossible. Hence x is odd and y is even. In $\mathbb{Z}[i]$ we can write $y^2 + 1 = (y + i)(y - i)$. If $d = \gcd(y + i, y - i)$, then d also divides $y + i - (y - i) = 2i = (1 + i)^2$ and $y + i + (y - i) = 2y$. If we assume that $d \neq 1$, we must have $d = 2, 1+i$ (or any of their respective associates).

We can immediately rule out $d = 2$, since $\frac{y+i}{2} \notin \mathbb{Z}[i]$. If $d = 1 + i$, then since $\mathbb{Z}[i]$ is closed under conjugation, at least one of the factors also contains $1 - i$, so that $(1 + i)(1 - i) = 2$ divides x. But this contradicts the fact that x is odd. Hence $d = 1$, so the factors are relatively prime.

Then by Lemma (3.12), $y+i$ and $y-i$ must both be perfect cubes (we do not need to consider any unit factor, since $\pm 1, \pm i$ can all be absorbed in the cube). For the first factor, we get, for some $c, d \in \mathbb{Z}$,

$$y+i = (c+di)^3 = c^3 + 3c^2di - 3cd^2 - d^3i = (c^3 - 3cd^2) + d(3c^2 - d^2)i$$

For this to hold, we must have $d(3c^2 - d^2) = 1$, i.e. $d = \pm 1, (3c^2 - d^2) = \pm 1$. If $d = 1$, we get the equation $3c^2 = 2$, which clearly has no integer solutions. Hence $d = -1$. This gives that $-(3c^2 - 1) = 1$, so that $c = 0$, and consequently $y + i = (-i)^3 = i$. Hence $y = 0$ and one solution is $(x, y) = (1, 0)$. The second factor must also be a cube, but since

$$y - i = \overline{y+i} = \overline{(c^3 - 3cd^2) + d(3c^2 - d^2)i} = (c^3 - 3cd^2) - d(3c^2 - d^2)i,$$

this does not give us any new information. Hence $(x, y) = (1, 0)$ is the only solution. □

Using basically the same argument as in the proof of Theorem (3.10), one can show that the ring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$ equipped with the function $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$ is a Euclidean domain. Its units are just ± 1, as in the usual integers. This fact can then be used to prove:

Theorem 3.14. *The only integer solutions to $y^2 = x^3 - 2$ is $(x, y) = (3, \pm 5)$.*

Proof. Observe that x must be odd in order to avoid $y^2 \equiv -2 \mod 4$. Hence y is odd as well. Write the equation as $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. Any element d in $\mathbb{Z}[\sqrt{-2}]$ that divides both factors must also divide the difference, $2\sqrt{-2} = -1(\sqrt{-2})^3$, so d must be of the form $(\sqrt{-2})^n$ for some $n = 0, 1, 2, 3$.

We can rule out the cases $n = 2, 3$, because if we divide $y + \sqrt{-2}$ by those values of d, we get $-\frac{1}{2}y - \frac{1}{2}\sqrt{-2}$ and $-\frac{1}{2} + \frac{y}{4}\sqrt{-2}$ respectively, neither of which belongs to $\mathbb{Z}[\sqrt{-2}]$. We can also rule out $n = 1$, because if $d = \sqrt{-2}$, then at least one of the factors also contains the conjugate $-\sqrt{-2}$, which means that the product $-(\sqrt{-2})^2 = 2$ divides x. This contradicts the fact that x is odd. So $d = 1$, and $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are relatively prime.

Hence both factors are cubes by Lemma (3.12), but as we saw in the previous proof, we only have to consider one of them. So assume that $(y + \sqrt{-2}) = (a + b\sqrt{-2})^3$ for $a, b \in \mathbb{Z}$. By expanding this and comparing coefficients, we get $b(3a^2 - 2b^2) = 1$, so that $b = \pm 1, (3a^2 - 2b^2) = \pm 1$. If $b = 1$, we get $3a^2 - 2 = 1$, which implies $a = \pm 1$ and consequently that $y = \pm 5$. If $b = -1$, we get $3a^2 - 2 = -1$ or equivalently $3a^2 = 1$, which clearly has no integer solutions. It is trivial to check that $(\pm 5)^2 + 2 = 27 = 3^3$, so that $(x, y) = (3, \pm 5)$ are the only possible solutions. □

The equation $y^2 = x^3 - 3$ can easily be shown to have no integer solutions using a congruence argument. However, if we want to show this using abstract algebraic methods, we cannot do as in the previous cases and just move on to the

"next" ring, $\mathbb{Z}[\sqrt{-3}]$. We saw earlier that every Euclidean domain has unique factorization, but in $\mathbb{Z}[\sqrt{-3}]$ we could write $4 = 2^2 = (1+\sqrt{-3})(1-\sqrt{-3})$, where all factors are irreducible. Hence $\mathbb{Z}[\sqrt{-3}]$ is not a Euclidean domain! It turns out that we have to be a bit more clever.

Definition 3.4. *The set* $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$, *where* $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ *is called the ring of Eisenstein integers.*

The complex number ω is a 3:rd root of unity, so that $\omega^3 = 1$, and consequently $\overline{\omega} = \omega^2$. Since ω and ω^2 are roots to the equation $x^2+x+1 = 0$, we also have the useful identity $\omega^2 = -1 - \omega$. Using an argument similar to the proof of Theorem (3.10), one can easily prove that $\mathbb{Z}[\omega]$ with the associated function $\delta(a + b\omega) = |a + b\omega|^2$ is a Euclidean domain. Its set of units is $\{\pm 1, \pm\omega, \pm\omega^2\}$, the complex 6:th roots of unity. We can derive a simple expression for δ as follows:

$$\begin{aligned}\delta(a + b\omega) &= |a + b\omega|^2 = (a + b\omega)(a + b\overline{\omega}) \\ &= (a + b\omega)(a + b\omega^2) = a^2 + ab\omega^2 + ab\omega + b^2\omega^3 \\ &= a^2 + ab(-1 - \omega + \omega) + b^2 = a^2 - ab + b^2\end{aligned}$$

One final important remark is that the Eisenstein primes are: $\lambda = 1-\omega$, integer primes that are $\equiv 2 \mod 3$, and elements π such that $\delta(\pi)$ is an integer prime $\equiv 1 \mod 3$. See for example [4]. Now we apply this to Mordell's equation.

Theorem 3.15. *The equation* $y^2 = x^3 - 3$ *has no integer solutions.*

Proof. By reducing modulo 8, we see that the only possibility is that both sides of $y^2 + 3 = x^3$ are $\equiv 3, 7 \mod 8$. This means that y is even and $x \equiv 3 \mod 4$.

Write the equation as $(y+\sqrt{-3})(y-\sqrt{-3}) = x^3$. If d is a common divisor of the two factors, then $d|2\sqrt{-3}$. Hence $d = 1, 2, \sqrt{-3}$. We can immediately rule out $d = 2$, since x is odd. Also, 3 does not divide $y + \sqrt{-3}$, so if $\sqrt{-3}$ divides $y + \sqrt{-3}$, it can only do so to a single power. Then $\sqrt{-3}$ divides the other factor to a single power as well (really the conjugate, $-\sqrt{-3}$, but the unit -1 can be absorbed in the cube). This means that $(\sqrt{-3})^2$ is the highest power that divides x^3, which is a contradiction. Hence $d = 1$, so the factors are relatively prime.

Then we can once again use Lemma (3.12) to deduce that both factors are of the form $u(c + d\omega)^3$ for some unit $u \in \mathbb{Z}[\omega]$. Three cases arise, depending on whether the unit is $1, \omega$ or ω^2. We can skip the negative units, since -1 can be absorbed in the cube. The first case gives

$$\begin{aligned}y + \sqrt{-3} &= (c + d\omega)^3 = c^3 + 3c^2d\omega + 3cd^2\omega^2 + d^3\omega^3 \\ &= c^3 + d^3 + 3c^2d\omega + 3cd^2(-1 - \omega) \\ &= (c^3 + d^3 - 3c^2d) + (3c^2 - 3cd^2)\frac{-1+\sqrt{-3}}{2} \\ &= \frac{2c^3 + 2d^3 - 3c^2d - 3cd^2}{2} + \frac{3c^2d - 3cd^2}{2}\sqrt{-3}\end{aligned}$$

Comparing the coefficients of $\sqrt{-3}$, we get the integer equation $3cd(c-d) = 2$, which has no solution since 2 is prime. The second case gives

$$\begin{aligned} y + \sqrt{-3} &= \omega(c + d\omega)^3 = \omega(c^3 + 3c^2d\omega + 3cd^2\omega^2 + d^3\omega^3) \\ &= 3cd^2 + (c^3 + d^3)\omega + 3c^2d\omega^2 \\ &= 3cd^2 + (c^3 + d^3)\omega + 3c^2d(-1 - \omega) \\ &= (3cd^2 - 3c^2d) + (c^3 - 3c^2d + d^3)\frac{-1 + \sqrt{-3}}{2} \\ &= \frac{-c^3 - 3c^2d + 6c^2d - d^3}{2} + \frac{c^3 - 3cd^2 + d^3}{2}\sqrt{-3} \end{aligned}$$

Comparing the coefficients of $\sqrt{-3}$ again, we get the equation $c^3 - 3c^2d + d^3 = 2$. By reducing $\mod 2$, we see that it is only solvable if c, d are both even. But then $8|(y + \sqrt{-3})$, which is impossible, since the resulting element is not in $\mathbb{Z}[\omega]$.

The last case is handled in a similar way, and gives $-(c^3 - 3cd^2 + d^3) = 2$, which again is only solvable if $c \equiv d \equiv 0 \mod 2$ and gives a similar contradiction. Hence there are no integer solutions. □

Before we look into the next equation, we need a deep result on cubic residues, discovered by Euler. As the name implies, we say that a is a cubic residue $\mod p$ if $x^3 \equiv a \mod p$ is solvable, and denote this by $(a/p)_3 = 1$. The proof however lies outside the scope of this thesis. The interested reader may consult [6] p.119.

Theorem 3.16. *Let p be a prime s.t. $p \equiv 1 \mod 6$. Then 2 is a cubic residue $\mod p$ if and only if p has a representation $p = A^2 + 27B^2$, where $A, B \in \mathbb{Z}$.*

Theorem 3.17. *The equation $x^3 + 2a^3 = y^2 + 3b^2$ has no integer solutions under the following assumptions: $ab \neq 0, a \not\equiv 1 \mod 3, b \not\equiv 0 \mod 3, b \equiv 0 \mod 2 \implies a \equiv 1 \mod 2$, and lastly 2 is a cubic residue of every prime $p \equiv 1 \mod 3$ dividing a.*

Proof. We view both sides of the equation as an integer N, which we will factor in primes. Possible prime divisors of N are 2, 3, common prime factors of x and a, primes $q \equiv 2 \mod 3$ and primes $p \equiv 1 \mod 3$ for which 2 is a cubic residue. We will show that the prime factorization of N contradicts our assumptions.

If $x^3 + 2a^3 \equiv 0 \mod 2$, then $y \equiv b \mod 2$. If $y \equiv b \equiv 0 \mod 2$, then $x^3 \equiv -2 \mod 4$ which is impossible. If instead $y \equiv b \equiv 1 \mod 2$, then $b \equiv \pm 1, \pm 3 \mod 8$ and $y \equiv \pm 1, \pm 3 \mod 8$, so that $y^2 + 3b^2 \equiv 4 \mod 8$. Also, $2a^3 \equiv 0, \pm 2 \mod 8$ holds for any a. Together, this yields $x^3 \equiv \pm 2, 4 \mod 8$, which is impossible.

We also cannot have $x^3 + 2a^3 \equiv 0 \mod 3$, since it implies $y \equiv 0 \mod 3$ and consequently $x^3 \equiv 3 - 2a^3 \equiv 3, 5 \mod 9$. This is impossible since perfect cubes

are $\equiv 0, \pm 1 \mod 9$

Hence, the remaining prime divisors will all be odd and $\equiv 1, 2 \mod 3$, or in other words $\equiv 1, 5 \mod 6$. First consider a prime $q_i \equiv 5 \mod 6$. Such a prime will also be $\equiv 5, 11 \mod 12$. Then, since

$$(-3/q) = (-1/q)(3/q) = \begin{cases} 1, & \text{if } q \equiv 1, 7 \mod 12 \\ -1, & \text{if } q \equiv 5, 11 \mod 12 \end{cases}$$

we can use Lemma (3.1) once again to conclude that any such prime must occur to an even power. Let $Q = \prod_i q_i^{\gamma_i}$, so that $Q^2 = \prod_i q_i^{2\gamma_i}$ (where $\gamma_i = min\{\alpha_i, \beta_i\}$, using the notation of lemma 3.1). Then $y^2 + 3b^2 = Q^2(y_1^2 + 3b_1^2)$, where every prime divisor of $(y_1^2 + 3b_1^2)$ is $\equiv 1 \mod 6$.

Let p_j be such a prime divisor. Regardless if $p_j | a$ or not, such a prime will have 2 as a cubic residue and hence be of the form $p_j = A_j^2 + 27B_j^2$ by Theorem (3.16). If $p_j | a$, it follows immediately from the assumption. If not, a will have a multiplicative inverse in $\mathbb{Z}_{p_j}$, say $\tilde{a}$. This allows us to multiply the congruence $x^3 \equiv -2a^3 \mod p_j$ by $(-\tilde{a})^3$ to obtain $(-\tilde{a}x)^3 \equiv 2 \mod p_j$, so that 2 is indeed a cubic residue.

Since $\sqrt{-3}, \sqrt{-27} \in \mathbb{Z}[\omega]$, we can factor our elements in $\mathbb{Z}[\omega]$ as $y_1^2 + 3b_1^2 = (y_1 + b_1\sqrt{-3})(y_1 - b_1\sqrt{-3})$, and $p_j = A_j + 27B_j = (A_j + B_j\sqrt{-27})(A_j - B_j\sqrt{-27})$. Hence we have

$$(y_1 + b_1\sqrt{-3})(y_1 - b_1\sqrt{-3}) = \prod_j (A_j + B_j\sqrt{-27})(A_j - B_j\sqrt{-27})$$

The factors in the right-hand side are irreducible, since they are conjugate factors of an integer prime that is $\equiv 1 \mod 3$. Because of this, each prime divisor of $y_1 + b_1\sqrt{-3}$ can only occur in one of the factors for each index j. Hence, by possibly changing notation $B_j \leftrightarrow -B_j$ for some indicies j, we can conclude that $\left(A_j + B_j\sqrt{-27}\right) \mid \left(y_1 + b_1\sqrt{-3}\right)$ for all j.

Since $\prod_j (A_j + B_j\sqrt{-27}) = C + D\sqrt{-27}$ for some integers C, D, we finally obtain

$$y_1 + b_1\sqrt{-3} = \pm\omega^m(C + D\sqrt{-27})$$

where $m = 0, \pm 1$. If $m = 0$, we get $y_1 + b_1\sqrt{-3} = \pm(C + 3D\sqrt{-3})$ which implies that $b_1 \equiv 0 \mod 3$ by comparing coefficients, regardless of the choice of sign. But since $b_1 | b$, we get that $b \equiv 0 \mod 3$ as well, which contradicts our assumptions. If $m = 1$, we get

$$(y_1 + b_1\sqrt{-3})\omega = (y_1 + b_1\sqrt{-3})\left(\frac{-1 + \sqrt{-3}}{2}\right) = \frac{-y_1 - 3b_1}{2} + \frac{y_1 - b_1}{2}\sqrt{-3}$$

which is not an element of $\mathbb{Z}[\omega]$ unless $y_1 \equiv b_1 \mod 2$, which implies $y \equiv b \mod 2$. But this has been excluded earlier. Similarly, the case $m = -1$ leads to

$$(y_1 + b_1\sqrt{-3})\omega^{-1} = (y_1 + b_1\sqrt{-3})\left(\frac{-1-\sqrt{-3}}{2}\right) = \frac{-y_1 - 3b_1}{2} + \frac{-y_1 - b_1}{2}\sqrt{-3}$$

which implies $y_1 \equiv b_1 \mod 2$ and consequently $y \equiv b \mod 2$. Since the last two cases led to contradictions in $\mathbb{Z}_2$, a negative sign of ω^m will not give us any new information. Hence there can be no integer solutions. □

The last equation of this section relies on a deep result similar to Theorem 3.16. In fact, it was also discovered by Euler. It is given as an exercise in [6], but the tools required for its proof are again outside the scope of this thesis.

Theorem 3.18. *Let p be a prime, $p \equiv 1 \mod 6$. Then 3 is a cubic residue mod p if and only if p has a representation $p = \frac{A^2+243B^2}{4}$, where $A, B \in \mathbb{Z}$.*

Theorem 3.19. *The equation $x^3 + 3a^3 = y^2 + 3b^2$ has no integer solutions where $k = 3(a^3 - b^2) \not\equiv 0 \mod 9$, unless that one of $b, b \pm (1-k)$ that is divisible by 3 is also divisible by 9.*

Proof. As in the previous theorem, we see both sides of the equation as an integer N which we will factor in primes. This time in Eisenstein primes, the irreducible elements in $\mathbb{Z}[\omega]$.

If $3|N$, then we must also have $x^3 \equiv 0 \mod 3$ and $y^2 \equiv 0 \mod 3$, but that implies $k = 3(a^3 - b^2) \equiv 0 \mod 9$, which contradicts our assumption. Hence $3 \nmid N$. This rules out λ since $3 = \lambda(2+\omega)$. This also means that $y^2 \equiv 1 \mod 3$, so that $x^3 \equiv 1 \mod 3$, and consequently $x^3 \equiv 1 \mod 9$. This will be used in the last step of the proof.

If $2|N$, then $y^2 + 3b^2 \equiv 0 \mod 2$ and consequently $y^2 \equiv b^2 \mod 2$. Hence 2 either divides both y and b, or none of them. In any case, 2 must occur to an even power (allowing zero). Similarly, any integer prime $q \equiv 5 \mod 6$ must also occur to an even power in N, since $(-3/q) = -1$, which allows us to use Lemma 3.1. Hence, if we let $d = \gcd(y, b)$, we can write $y^2 + 3b^2 = d^2(y_1^2 + 3b_1^2)$, where $\gcd(y_1, b_1) = 1$. This also means that all integer prime factors of $y_1^2 + 3b_1^2$ (except 2, if both y_1 and b_1 are odd) are $\equiv 1 \mod 6$ (the other kinds of primes must all occur to an even power and hence be included in d^2).

Any such integer prime can be split into conjugate prime factors $a + b\omega, a + b\omega^2$ in $\mathbb{Z}[\omega]$. By possibly multiplying by a unit, the factors can be written in primary form, meaning that $a \equiv 1 \mod 3, b \equiv 0 \mod 3$ (see [4]). We divide all such primes into two groups, depending on whether they have 3 as a cubic residue or not. Those that do not have 3 as a cubic residue will be denoted $p_i = s_i + t_i\omega$ or $p_i = s_i + t_i\omega^2$, and they must occur to a power which is a multiple of 3. The primes that have 3 as a cubic residue can be written in the

special form $\hat{p_i} = \frac{A_i^2+243B_i}{4}$ by Theorem 3.18, but we have no control over the powers to which they occur.

As before, we can factor $y_1^2 + 3b_1^2$ as $(y_1 + b_1\sqrt{-3})(y_1 - b_1\sqrt{-3})$. Depending on whether y_1 and b_1 are incongruent $\mod 2$ or both odd, we have either $gcd(y_1 + b_1\sqrt{-3}, y_1 - b_1\sqrt{-3}) = 1$ or $gcd\left(\frac{y_1+b_1\sqrt{-3}}{2}, \frac{y_1-b_1\sqrt{-3}}{2}\right) = 1$. In the first case, the greatest common divisor g has to divide $2y_1$ and $2b_1\sqrt{-3}$. However, $g \neq 2$ since none of the factors is divisible by 2, and $g \neq \sqrt{-3}$ since assuming otherwise implies that $3|N$, which we have ruled out. The only remaining option is then that g divides both y_1 and b_1, but that is impossible since $y_1 \not\equiv b_1 \mod 2$. In the case when y_1 and b_1 are both odd, we still have $g \neq 2$ and $gcd(y_1, b_1) = 1$. However, both factors will be divisible by 2, so we get $gcd\left(\frac{y_1+b_1\sqrt{-3}}{2}, \frac{y_1-b_1\sqrt{-3}}{2}\right) = 1$. Since these two cases will differ only in notation (a factor of 2), and all the same conclusions will follow, we choose to only write out the details of the first case.

To sum things up, we have:

$$\begin{aligned} N = x^3 + 3a^3 = y^2 + 3b^2 = d^2(y_1^2 + 3b_1^2) \\ = d^2 \prod_i p_i^{3n_i} \prod_i \hat{p_i}^{m_i} \end{aligned}$$

Upon cancelling d^2 and expanding, this is equivalent to

$$\begin{aligned} (y_1 + b_1\sqrt{-3})(y_1 - b_1\sqrt{-3}) = \prod_i (s_i + t_i\omega)^{3n_i}(s_i + t_i\omega^2)^{3n_i} \\ \times \prod_i \left(\frac{A_i + 9B_i\sqrt{-3}}{2}\right)^{m_i} \left(\frac{A_i - 9B_i\sqrt{-3}}{2}\right)^{m_i} \end{aligned} \tag{3.1}$$

Note that the product does not contain ω, even though every p_i must be multiplied by some unit in order to be in primary form. For whatever power n_i of ω needed to put $s_i + t_i\omega$ in primary form, the same power of $\overline{\omega} = \omega^2$ is needed to put the conjugate $s_i + t_i\omega^2$ in primary form. Hence, the product contains a factor of $\omega^{n_i}(\omega^2)^{n_i} = (\omega^3)^{n_i} = 1$ for each i.

Because the factors on the left-hand side of Equation (3.1) are relatively prime, any prime occurring in the right-hand side can only divide one of those factors, which means that the conjugate of every such prime must divide the other. Hence, by possibly replacing ω with ω^2 or B_i with $-B_i$ for some indicies i, we can conclude

$$(y_1 + b_1\sqrt{-3}) = \pm\omega^n \prod_i (s_i + t_i\omega)^{3n_i} \prod_i \left(\frac{A_i + 9B_i\sqrt{-3}}{2}\right)^{m_i} \tag{3.2}$$

Similarly for the conjugates. Some simple but tedious calculations show that:

$$\begin{aligned} &\prod (s_i + t_i\omega)^3 = s + t\omega, \\ &\prod \left(\frac{A_i + 9B_i\sqrt{-3}}{2} \right) = \left(\frac{A + B\sqrt{-3}}{2} \right) \end{aligned} \tag{3.3}$$

where $t, B \equiv 0 \mod 9$, and again similarly for their conjugates. Another tedious calculation reveals that

$$(s + t\omega) \left(\frac{A + 9B\sqrt{-3}}{2} \right) = \left(\frac{C + D\sqrt{-3}}{2} \right)$$

where $D \equiv 0 \mod 9$, and yet again similarly for the conjugates. We can now finally conclude that

$$(y_1 + b_1\sqrt{-3}) = \pm\omega^n \left(\frac{C + D\sqrt{-3}}{2} \right)$$

where $n = 0, 1, 2$. Three distinct cases arise (it turns out that the choice of sign does not matter).

In the first case $n = 0$, we get

$$y_1 + b_1\sqrt{-3} = \frac{C + D\sqrt{-3}}{2}$$

which implies $2b_1 \equiv 0 \mod 9$, and consequently $b \equiv 0 \mod 9$. The second case gives

$$\begin{aligned} y_1 + b_1\sqrt{-3} &= \left(\frac{-1 + \sqrt{-3}}{2} \right) \left(\frac{C + D\sqrt{-3}}{2} \right) \\ &= \frac{-C - 3D}{4} + \frac{C - D}{4}\sqrt{-3} \end{aligned}$$

which implies $4y_1 \equiv -C - 3D \equiv -C \mod 9$ and $4b_1 \equiv C - D \equiv C \mod 9$, so that $4(y_1 + b_1) \equiv -C + C \equiv 0 \mod 9$. This in turn implies $y + b \equiv 0 \mod 9$. In the last case, we get

$$\begin{aligned} y_1 + b_1\sqrt{-3} &= \left(\frac{-1 - \sqrt{-3}}{2} \right) \left(\frac{C + D\sqrt{-3}}{2} \right) \\ &= \frac{-C + 3D}{4} + \frac{-C - D}{4}\sqrt{-3} \end{aligned}$$

which implies $4y_1 \equiv -C \mod 9$, $4b_1 \equiv -C \mod 9$, and consequently $4(b_1 - y_1) \equiv 0 \mod 9$. This in turn implies $b - y \equiv 0 \mod 9$.

Finally, since $x^3 \equiv 1 \mod 9$, we see that $y^2 \equiv 1 + k \mod 9$. Also, since $-3k, k^2 \equiv 0 \mod 9$, we can add them to the congruence to obtain $y^2 \equiv 1 + k - 3k + k^2 \equiv (1 - k)^2 \mod 9$, which implies $y \equiv \pm(1 - k) \mod 9$. Combining this with what we found in the different cases above, the conclusion follows. □

4 Fermat's Equation for $n = 3$

The equation $x^3+y^3 = z^3$ has at least been known since Fermat, who claimed to have a proof using infinite descent. However, as with most of Fermat's claims, it is disputed whether that was actually the case. The first known proof was due to Euler, published in 1770. Unfortunately, Euler's argument contained a small flaw, but it was realized by other mathematicians that this flaw could be fixed using methods that Euler was well aware of. In this section however we take another approach and prove the more general result, that

$$x^3 + y^3 = uz^3 \tag{4.1}$$

has no solution, where $x, y, z, u \in \mathbb{Z}[\omega]$ and u is a unit.

Most of the work is done by proving a series of lemmas, relying on properties of the irreducible element $\lambda = 1 - \omega$. The main theorem is then proved using a variant of infinite descent. Following [6], we introduce some new notation before we start.

Definition 4.1. *For a prime element p we write $ord_p a = n$ if $a = p^n a_1$, where $p \nmid a_1$. The function $f(x) = ord_p(x)$ is called the order function.*

It is easily checked that the following holds:

$$\begin{aligned}
&\mathrm{ord}_p(a) \geqslant 0, \text{with equality only if } p \nmid a \\
&\mathrm{ord}_p(a \pm b) \geqslant \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \\
&\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \\
&\mathrm{ord}_p(a^n) = n\ \mathrm{ord}_p(a)
\end{aligned}$$

Here equality holds in the second property as long as $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$. For ordinary integers, this is basically the same as the notation $p^n||a$ introduced in Chapter 3.1. For a more thorough discussion of the ord function in general domains and its applications to Mordell's Equation, see Chapter 6 of [2].

Lemma 4.1. *Every element in $\mathbb{Z}[\omega]$ is $\equiv 0, \pm 1 \mod \lambda$.*

Proof. It is clear that $a + b\omega \equiv a + b \mod \lambda$. Since $3 = \lambda(2 + \omega)$, we can write this as

$$a + b\omega = a + b + \lambda k_1 = a + b + 3k_2$$

for some $k_1, k_2 \in \mathbb{Z}[\omega]$, so that $a + b\omega \equiv a + b \mod 3$ as well. Since $a + b$ will obviously be congruent to $0 \pm 1 \mod 3$ for any integers a, b, the result follows. □

Lemma 4.2. *Equation* (4.1) *has no solution s.t.* $\lambda \nmid xyz$.

Proof. The assumption gives that λ divides none of x, y, z. We claim that $x \equiv 1 \mod \lambda \implies x^3 \equiv 1 \mod \lambda^4$. If $x = 1 + \lambda t$, then

$$\begin{aligned} x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) &= \lambda t(1-\omega+\lambda t)(1-\omega^2+\lambda t) \\ &= \lambda t(\lambda+\lambda t)((1+\omega)\lambda+\lambda t) = \lambda^3 t(1+t)(1+\omega+t) \\ &= \lambda^3 t(1+t)(t-\omega^2) \end{aligned}$$

We have that $\omega \equiv 1 \mod \lambda, t \equiv 0, \pm 1 \mod \lambda$, and we need to show that $\lambda^3 t(1+t)(t-\omega^2) \equiv 0 \mod \lambda^4$ holds in all cases.

First assume that $t \equiv 1$, so that $\omega = \lambda s_1 + 1, t = \lambda s_2 + 1$. Then we get

$$\begin{aligned} \lambda^3 t(1+t)(t-\omega^2) &= \lambda^3(\lambda s_2+1)(1+\lambda s_2+1)(\lambda s_2+1-(\lambda s_1+1)^2) \\ &= \lambda^4(\lambda s_2+1)(\lambda s_2+2)(s_2-2s_1-\lambda s_1^2) \equiv 0. \end{aligned}$$

If instead $t = \lambda s_2 - 1$, we get

$$\begin{aligned} \lambda^3 t(1+t)(t-\omega^2) &= \lambda^3(\lambda s_2-1)(1+\lambda s_2-1)(\lambda s_2-1-(\lambda s_1+1)^2) \\ &= \lambda^4 s_2(\lambda s_2-1)(\lambda(s_2-2s_1-\lambda s_1^2)-2) \equiv 0. \end{aligned}$$

Finally, if $t = \lambda s_2$,

$$\begin{aligned} \lambda^3 t(1+t)(t-\omega^2) &= \lambda^3(\lambda s_2)(1+\lambda s_2)(\lambda s_2-(\lambda s_1+1)^2) \\ &= \lambda^4 s_2(1+\lambda s_2)(\lambda(s_2-2s_1-\lambda s_1^2)-1) \equiv 0. \end{aligned}$$

Now assume that the equation $x^3+y^3 = uz^3$ holds. Then, by reducing $\mod \lambda^4$, we get $\pm 1 \pm 1 \equiv \pm u \mod \lambda^4$, or in other words $\pm 1 \pm 1 \pm u = k\lambda^4$. We claim that $\lambda \nmid 2$, because if we assume that $(a+b\omega)\lambda = 2$ and solve for a, b we get a system of equations lacking integer solutions. Now, taking the ord_λ function of both sides, we obtain

$$\mathrm{ord}_\lambda(\pm 2 \pm u) = \mathrm{ord}_\lambda(k\lambda^4)$$

and consequently

$$\min\{\mathrm{ord}_\lambda(\pm 2), \mathrm{ord}_\lambda(\pm u)\} = \mathrm{ord}_\lambda k + 4$$

so that $0 = \mathrm{ord}_\lambda k + 4$, since none of $\pm 2, \pm u$ are divisible by λ. This is clearly impossible, and the same argument of course applies if we choose signs so that $\pm 1 \pm 1 = 0$. Hence the equation has no solutions. □

Lemma 4.3. *If equation* (4.1) *has a solution s.t.* $\lambda \nmid xy$ *and* $\lambda | z$, *then* $\lambda^2 | z$.

Proof. By the previous lemma, we can reduce the equation $\mod \lambda^4$ to obtain $\pm 1 \pm 1 \equiv uz^3 \mod \lambda^4$. First assume that $0 \equiv uz^3 \mod \lambda^4$ so that $uz^3 = k\lambda^4$. Then we can apply the ord_λ function to both sides to obtain

$$\mathrm{ord}_\lambda u + 3\mathrm{ord}_\lambda z = \mathrm{ord}_\lambda k + 4\mathrm{ord}_\lambda \lambda$$

and consequently

$$3\text{ord}_\lambda z = \text{ord}_\lambda k + 4 \geqslant 4$$

which implies that $\text{ord}_\lambda z \geqslant 2$, or in other words, $\lambda^2 | z$. The other case $uz^3 = k\lambda^4 \pm 2$ leads to

$$3\text{ord}_\lambda z = \min\{\text{ord}_\lambda(k\lambda^4), \text{ord}_\lambda(\pm 2)\} = \min\{\text{ord}_\lambda k + 4, 0\} = 0$$

so that $\text{ord}_\lambda z = 0$, or in other words, $\lambda \nmid z$. But this contradicts our assumption. □

The crucial step is the following:

Lemma 4.4. *If equation 4.1 has a solution s.t. $gcd(x, y) = 1$, $\lambda \nmid xy$ and $ord_\lambda z \geqslant 2$, then there exist $x_1, y_1, z_1, u_1 \in \mathbb{Z}[\omega]$, u_1 a unit, s.t $x_1^3 + y_1^3 = u_1 z_1^3$, $\lambda \nmid x_1 y_1$ and $ord_\lambda z_1 = ord_\lambda z - 1$.*

Proof. Assume that Equation (4.1) admits a solution satisfying our assumptions. The polynomial $p(x) = x^3 + y^3$ has zeros $x = -y, -\omega y, -\omega^2 y$, which allows us to write the equation as $(x + y)(x + \omega y)(x + \omega^2 y) = uz^3$ by the factor theorem. Since $\lambda^2 | z$, we have that $\text{ord}_\lambda(uz^3) = 3\text{ord}_\lambda z \geqslant 6$. Then, by possibly replacing y by ωy or $\omega^2 y$, we can conclude that $\text{ord}_\lambda(x + y) \geqslant 2$. Since $\text{ord}_\lambda(1 - \omega) = 1$, we get that

$$\begin{aligned}\text{ord}_\lambda(x + \omega y) &= \text{ord}_\lambda(x + y - (1 - \omega)y) = \min\{\text{ord}_\lambda(x + y), \text{ord}_\lambda(1 - \omega)y\} \\ &= \min\{\text{ord}_\lambda(x + y), 1 + \text{ord}_\lambda y\} = \min\{\text{ord}_\lambda(x + y), 1\} = 1\end{aligned}$$

and similarly

$$\begin{aligned}\text{ord}_\lambda(x + \omega^2 y) &= \text{ord}_\lambda(x + y - (1 - \omega)(1 + \omega)y) \\ &= \min\{\text{ord}_\lambda(x + y), \text{ord}_\lambda(1 - \omega) + \text{ord}_\lambda(1 + \omega) + \text{ord}_\lambda y\} \\ &= \min\{\text{ord}_\lambda(x + y), 1\} = 1\end{aligned}$$

Hence,

$$\begin{aligned}&\text{ord}_\lambda((x + y)(x + \omega y)(x + \omega^2 y)) \\ &= \text{ord}_\lambda(x + y) + \text{ord}_\lambda(x + \omega y) + \text{ord}_\lambda(x + \omega^2 y) \\ &= \text{ord}_\lambda(x + y) + 2\end{aligned}$$

so that

$$\text{ord}_\lambda(x + y) = 3\text{ord}_\lambda z - 2$$

An irreducible element $\pi \in \mathbb{Z}[\omega]$ different from λ cannot divide $(x + y)$ and $(x + \omega y)$. If that were the case, π would also have to divide $(x + y) - (x + \omega y) = (1 - \omega)y = \lambda y$ and $(x + y) + (x + \omega y) = 2x + (1 + \omega)y$, so that $\pi | x, \pi | y$ (here we used that 2 is prime in $\mathbb{Z}[\omega]$). That is of course impossible since we assumed

$\gcd(x, y) = 1$. Hence the only irreducible that divides both factors is λ, so that $\gcd(x + y, x + \omega y) = \lambda$. Similarly for the other pairs of factors.

Then, by unique factorization, we can write:

$$\begin{aligned} x + y &= u_1\alpha^3\lambda^{3ord_\lambda z-2},\ \lambda \nmid \alpha \\ x + \omega y &= u_2\beta^3\lambda,\ \lambda \nmid \beta \\ x + \omega^2 y &= u_3\gamma^3\lambda,\ \lambda \nmid \gamma \end{aligned}$$

where u_1, u_2, u_3 are some units. Multiplying the second equation by ω and the third by ω^2, the left hand sides become

$$(x + \omega y)\omega = x\omega + y\omega^2 = x\omega + (-1 - \omega)y = -y + (x - y)\omega$$

and

$$(x + \omega^2 y)\omega^2 = x\omega^2 + y\omega^4 = x(-1 - \omega) + y\omega = -x + (-x + y)\omega$$

Then, upon adding the three equations, the left hand sides cancel out, so we get:

$$u_1\alpha^3\lambda^{3ord_\lambda z-2} + u_2\omega\beta^3\lambda + u_3\omega^2\gamma^3\lambda = 0$$

or if we cancel λ,

$$u_1\alpha^3\lambda^{3(ord_\lambda z-1)} + u_2\omega\beta^3 + u_3\omega^2\gamma^3 = 0$$

Now let $z_1 = \alpha\lambda^{\mathrm{ord}_\lambda z-1}, \beta = x_1, \gamma = y_1$. Then $u_1 z_1^3 + u_2\omega x_1^3 + u_3\omega^2 y_1^3 = 0$, where $\gcd(x_1, y_1) = 1$. Since the units in $\mathbb{Z}[\omega]$ form a group under multiplication, we can multiply by $(u_2\omega)^{-1}$ to obtain

$$x_1^3 + \epsilon_1 y_1^3 = \epsilon_2 z_1^3$$

where ϵ_1, ϵ_2 are some other units.

By the proof of Lemma (4.2), any cube that is not divisible by λ will be $\equiv 1 \mod \lambda^2$. Since $\lambda | z_1$, so that $\lambda^2 | z_1^3$, we can reduce the equation $\mod \lambda^2$ to obtain $\pm 1 \pm \epsilon_1 \equiv 0 \mod \lambda^2$. Looking at possible sums and differences of units in $\mathbb{Z}[\omega]$, we see that the only possibility is that $\pm 1 \pm \epsilon_1 = 0$, so that $\epsilon_1 = \pm 1$. Since -1 can be absorbed in the cube, we finally arrive at

$$x_1^3 + y_1^3 = \epsilon_2 z_1^3$$

where $ord_\lambda z_1 = ord_\lambda(\alpha\lambda^{ord_\lambda z-1}) = ord_\lambda z - 1$. This finishes the proof. □

With all the lemmas done, the proof of the main result is now an easy task.

Proof. Assume that $x^3 + y^3 = uz^3$ holds. If it should happen that λ divides all of x, y, z to some powers n_1, n_2, n_3, then we can divide the equation by $\lambda^{min\{n_1,n_2,n_3\}}$ to arrive at one of the following cases: If $\lambda \nmid xyz$, then no solution exist by Lemma (4.2). If $\lambda \nmid xy$, but $\lambda|z$, Lemma (4.3) gives that $\lambda^2|z$. But then Lemma (4.4) can be applied to construct another solution with a "smaller" value of z. This creates an infinite decreasing sequence of positive integers, $\{ord_\lambda z_i\}_{i=1}^{\infty}$, which contradicts the well-ordering axiom. Hence no solution can exist.

The last case where $\lambda \nmid yz, \lambda|x$ is more interesting. By the proof of Lemma (4.2), any cube not divisible by λ will be $\equiv 1 \mod \lambda^3$. Then we can reduce the equation $x^3 + y^3 = uz^3 \mod \lambda^3$ to obtain $1 \equiv u \mod \lambda^3$. Again, looking at possible sums and differences of units, we see that $u = \pm 1$ is the only possibility. But then we can rewrite the original equation as $(\pm z)^3 + (-y)^3 = x^3$, and we are back in the previous case.

Hence Equation (4.1) has no solutions in the ring of Eisenstein integers, and consequently not in ordinary integers either. □

5 Appendix: k-values

In chapter 3.1, we proved that Mordells equation lacks integer solutions for certain values of k, depending on some integer parameters. In this appendix we explicitly compute some of those values. Most of the computations were made numerically in Python. For example, to find some k-values from Theorem (3.6), the following code was used:

```
primes=[i for i in range(2,100) if (isprime(i)==True)]
primes=[p for p in primes if (p%8==5 or p%8==7)] # list of p = 5,7 mod 8
A=[i for i in range(-30,30) if (i%8==4)] # list of a = 4 mod 8
B=[]
for i in range(30):
    if i%2==1: # b odd
        for p in primes:
            if i%p==0: # b has no prime factor p = 5,7 mod 8
                break
        else:
            B.append(i)
for a in A:
    for b in B:
        k=-1*a**3-2*b**2
        if abs(k)<100:
            print('(a,b)=({},{}) gives k={}'.format(a,b,k))
```

Theorem 3.3:

a	b	k
1	0	-5
1	1	23
5	1	-73
29	4	11

Theorem 3.4:

a	b	k
-7	1	47
-3	-1	-33
-3	0	-17
-1	-1	-9

Theorem 3.5:

a	b	k
2	1	-6
-2	1	10
4	1	-62
-4	1	66
2	7	90
4	7	34
10	23	-58

Theorem 3.6:

a	b	k
-4	1	62
-4	3	46
-4	9	-98
4	1	-66
4	3	-82

Theorem 3.8:

a	b	c	k
-5	6	1	-89
-5	8	1	-61
-1	2	1	5
-1	4	1	17
-1	6	1	37
-1	8	1	65
-1	2	3	39
-1	4	3	75
3	2	1	-23
3	4	1	-11
3	6	1	9
3	8	1	37

References

[1] Burton D., Elementary Number Theory, 7th edition, McGraw Hill Education (2011)

[2] Clarke, P., Number Theory: A Contemporary Introduction (pdf, avaliable at http://math.uga.edu/ pete/4400FULL.pdf)

[3] Dickson, L.E., History of the Theory of Numbers, Volume II: Diophantine Analysis, Chelsea Publishing Company (1952)

[4] Hall, M. Jr., Some Equations $y^2 = x^3 - k$ Without Integer Solutions, J Lond. Math. Soc., 28, p.379-383 (1953)

[5] Hungerford, T. W., Abstract Algebra: An Introduction, 2nd edition, Brooks/Cole (1997)

[6] Ireland K. Rosen M., A Classical Introduction to Modern Number Theory, 2nd edition, Springer (1998)

[7] Mordell, L.J, Diophantine Equations, Academic Press (1969)